Oak Wood School

# Data Protection Policy 2025-26

*We dream, we learn, we grow*

**CONTENTS**

Policy

Appendices:

1. Data Breach Policy
2. Data Retention Policy
3. Electronic Information and Communications Policy
4. Freedom of Information Policy and Publication Scheme
5. Privacy Notice for Pupils and Parents
6. Privacy Notice for Governors and Volunteers
7. Privacy Notice for Job Applicants
8. Privacy Notice for Visitors and contractors
9. Privacy Notice for Staff
10. Information Security Policy

## Data Protection Policy

### Introduction

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Staff is defined by employees, governors, trustees and volunteers. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up and including dismissal depending on the seriousness of the breach.

### Section 1 – Definitions

| | |
|---|---|
| **Personal Data** | **Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.**<br><br>**Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.**<br><br>**Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.** |
| **Special Category Data and Data Relating to Criminal** | Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade |

| | |
|---|---|
| **Convictions and Offences** | union membership, physical and mental health, sexuality and biometric or genetic data.<br><br>Personal data relating to criminal offences and convictions is included here for the purposes of this policy. This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures. |
| **Data Subject** | An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees. |
| **Data Controller** | The organisation storing and controlling such information (i.e., the School) is referred to as the Data Controller. |
| **Processing** | Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties. |
| **Automated Processing** | Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.<br><br>An example of automated processing includes profiling and automated decision making. Automatic decision-making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision-making is prohibited except in exceptional circumstances. |
| **Data Protection Impact Assessment (DPIA)** | DPIAs are a tool used to identify risks in data processing activities with a view to reducing them. |
| **Data Breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. |
| **Pseudonymised** | The process by which personal data is processed in such a way that that it cannot be used to identify an individual |

without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual.

## Section 2 – When can the School Process Personal Data?

### Data Protection Principles

The School are responsible for and adhere to the principles relating to the processing of personal data as set out in the UK GDPR. The principles the School must adhere to are set out below.

### Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The School only collect, process and share personal data fairly and lawfully and for specified purposes.

The School must have a specified purpose for processing personal data and special category data as set out in the UK GDPR.

Before the processing starts for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).

*Personal Data*

The School may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;

- For the purposes of the School's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

*Special Category Data*

The School may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing is necessary for archiving, statistical or research purposes.

The School identifies and documents the legal grounds being relied upon for each processing activity.

*Criminal Record Data*

Criminal records data is processed, also identify a lawful condition for processing that data and document it.

*Consent*

Where the School relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent is needed in cases of processing special category data and requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their non-special category personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

In cases of processing special category data and explicit consent, the School will normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

**Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes**

Personal data will not be processed in any manner that is incompatible with the legitimate purposes specified.

The School will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

**Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed**

The School will only process personal data when our obligations and duties require us to. We will not collect excessive data and will ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the School shall delete or anonymise the data. Please refer to the School's Data Retention Policy for further guidance.

**Principle 4: Personal data must be accurate and, where necessary, kept up to date**

The School will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the School.

**Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed**

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The School will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the School's Retention Policy for further details about how the School retains and removes data.

**Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage**

In order to ensure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where the School replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access on both hard copy and electronic files (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;

- Ensuring personal data is accurate and suitable for the process for which it is processed.

The School follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The School will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Full details on the School's security measures are set out in the School's Information Security Policy.

*Sharing Personal Data*

The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services;
- Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities for example, the Local Authority, Ofsted or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the School shall be clearly defined within written notifications including details and the basis for sharing the data.

*Transfer of Data Outside the European Economic Area (EEA)*

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

The School will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the School's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

*Transfer of Data Outside the UK*

The School may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection. Alternatively, the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, Standard Contractual Clauses or compliance with an approved code of conduct.

## Section 3 – Data Subject's Rights and Requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.
The rights data subjects have in relation to how the School handle their personal data are set out below: -

(a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

(b) Receive certain information about the School's processing activities;

(c) Request access to their personal data that we hold (see "Subject Access Requests" at Appendix 1);

(d) Prevent our use of their personal data for marketing purposes;

(e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(f) Restrict processing in specific circumstances;

(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) Request a copy of an agreement under which personal data is transferred outside of the EEA;

(i) Object to decisions based solely on automated processing;

(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(l) Make a complaint to the supervisory authority, which is the Information Commissioner in England and Wales https://ico.org.uk/global/contact-us/; and

(m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the School to verify the identity of the individual making the request.

**Direct Marketing**

The School are subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The School will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The School will promptly respond to any individual objection to direct marketing.

**Employee Obligations**

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the School in the course of their employment or engagement. If so, the School expects those employees to help meet the School's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example, by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction Please refer to the School's Information Security Policy for further details about our security processes;
- Not remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;
- Not store personal information on local drives.

## Section 4 - Accountability

The School will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

The School have taken the following steps to ensure and document UK GDPR compliance:-

### Data Protection Officer (DPO)

Please find below details of the School's Data Protection Officer: -

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

(a) If you are unsure of the lawful basis being relied on by the School to process personal data;

(b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);

(c) If you need to draft privacy notices or fair processing notices;

(d) If you are unsure about the retention periods for the personal data being processed but would refer you to the School's Data Retention Policy in the first instance;

(e) If you are unsure about what security measures need to be put in place to protect personal data;

(f) If there has been a personal data breach and would refer you to the procedure set out in the School's Data Breach Policy;

(g) If you are unsure on what basis to transfer personal data outside the EEA;

(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if

you plan to use personal data for purposes other than what it was collected for;

(j) If you plan to undertake any activities involving automated processing or automated decision making;

(k) If you need help complying with applicable law when carrying out direct marketing activities;

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

**Personal Data Breaches**

The UK GDPR requires the School to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. Please refer to our Data Breach policy. This is available in the staff share folder.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches who is the Director of Finance and Operations or your DPO.

**Transparency and Privacy Notices**

The School will provide detailed, specific information to data subjects. This information will be provided through the School's privacy notices and/or fair processing notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. The School's privacy notices are tailored to suit the data subject and set out information about how the School use their data.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR. This includes the identity of the Data Protection Officer, the School's contact details, how and why we will use, process, disclose, protect and retain personal data. This information will be provided within our privacy notices.

When personal data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, we will provide the data subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and where relevant, be written in a form understandable by those defined as “children” under the UK GDPR.

**Privacy by Design**

The School adopt a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the School takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

**Data Protection Impact Assessments (DPIAs)**

In order to achieve a privacy by design approach, the School conduct DPIAs for any new high risk technologies or programmes being used by the School which could affect the processing of personal data.. The School carries out DPIAs when required by the UK GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data; and
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- Details of what types of data are shared;
- Steps taken by the third party and the school in order to protect data;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

**Record Keeping**

The School are required to keep full and accurate records of our data processing activities. These records include: -

- The name and contact details of the School;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;

- Details of the School's processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

**Training**

The School will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws. The school will carry out adequate training with all staff on an annual basis.

**Audit**

The School, through its Data Protection Officer, regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place regularly in order to review use of personal data.

**Related Policies**

Staff should refer to the following policies that are related to this Data Protection Policy:

-

- Data Breach Policy
- Data Retention Policy
- Electronic Information and Communications Policy
- Freedom of Information Policy
- Privacy Notice for Pupils and Parents
- Privacy Notice for Governors and Volunteers
- Privacy Notice for Job Applicants
- Privacy Notice for Visitors and contractors
- Privacy Notice for Staff
- Information Security Policy

These policies are also designed to protect personal data and can be found at in the staff shared Policy folder.

**Monitoring**

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

## Appendix 1 – Subject Access Requests

Under Data Protection Law, data subjects have a general right to find out whether the School hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the School are undertaking. It is designed to assist individuals in understanding how and why we are using their data and to check that we are doing so lawfully. The main provisions are to be found in Articles 12 and 15 of the UK GDPR and Section 45 of the Data Protection Act 2018.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the School at potentially significant risk and so the School takes compliance with this policy very seriously.

A data subject has the right to be informed by the School of the following: -

(a) Confirmation that their data is being processed;

(b) Access to their personal data;

(c) A description of the information that is being processed;

(d) The purpose for which the information is being processed;

(e) The recipients/class of recipients to whom that information is or may be disclosed;

(f) Details of the School's sources of information obtained;

(g) In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and

(h) Other supplementary information.

Dealing with a SAR is time critical and must be prioritised. Other than in exceptional cases, we will have only one month in which to respond to a SAR and even if an extension of the time limit is permitted, the individual must still be informed within that month of the fact that the request will take longer to process and the reasons for the delay. Failure to deal with a SAR within that period could leave us open to the possibility of being fined by the ICO.

All staff must be aware of the potential for receiving a SAR and the importance of dealing with such as request as a matter of urgency.

Anyone within the School may receive a SAR. It does not need to be made to a nominated person or even to a person responsible for dealing with either the data subject or information of that type. It will be equally as valid if sent to anyone within the school.

If you receive a SAR, please contact the Director of Fiinance and Operations. A request for information does not need to mention that it is a SAR provided that it is clear that it is an individual asking for their own personal data. There is no specified wording and it does not have to be on an official form. A SAR does not need to be in writing and can be made verbally, by post, by email or even using social media where relevant.

**How to Recognise a Subject Access Request**

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the School process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text, social media) or verbally (e.g., during a telephone conversation or meeting). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the School hold about me' would constitute a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data and not information relating to other people.

**How to Make a Data Subject Access Request**

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the School to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is

unclear/vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

If a request is made verbally, we will ensure we follow this up with something in writing to confirm what has been requested and outline the timeframe for dealing with the request.

**What to do When You Receive a Data Subject Access Request**

All data subject access requests should be immediately directed to the Director of Finance and Operations who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the School must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual. If ever in doubt, please refer the request to the Director of Finance and Operations.

**Acknowledging the Request**

When receiving a SAR the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the School may ask for:

- proof of ID (if needed);
- further clarification about the requested information if it is not clear what information is required;
- if it is not clear where the information shall be sent, the School must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The School should work with their DPO in order to create the acknowledgment.

**Verifying the Identity of a Requester or Requesting Clarification of the Request**

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the School may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The School shall let the requestor

know as soon as possible where more information is needed before responding to the request.

When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding pauses when further information is requested and does not restart until sufficient clarification is provided.

In both cases, the school will be unable to comply with the request if they do not receive the additional information.

**Requests Made by Third Parties or on Behalf of Children**

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The School may also require proof of identity in certain circumstances.

If the School is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;

- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The School may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

**Fee For Responding to a SAR**

The School will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the School will inform the requester why this is considered to be the case and that the School will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

**Time Period for Responding to a SAR**

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received. Where the school may be required to get consent from a pupil, the time period will not start until consent is received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular

nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

**School Closure Periods**

The school may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because no one will be on site to comply with the request during this period. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e., until a time when we receive the request). However, if we can acknowledge the request, we may still not be able to deal with it until the School re-opens. The School will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

**Information to be Provided in Response to a Request**

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
    - to request that the Company rectifies, erases or restricts the processing of his personal data; or
    - to object to its processing;
    - to lodge a complaint with the ICO;
    - where the personal data has not been collected from the individual, any information available regarding the source of the data;
    - any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical

terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the School are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the School have one month in which to respond the School is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

Therefore, the School is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The School is not allowed to amend or delete data to avoid supplying the data.

**How to Locate Information**

The personal data the School need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the School may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- safeguarding systems (such as CPOMS, MyConcern);
- MIS system (such as SIMS, Bromcom, Arbor);
- occupational health records;
- pensions data;
- share scheme information;
- insurance benefit information.

The School should search these systems using the individual's name, initials, employee number or other personal identifier as a search determinant.

**Protection of Third Parties - Exemptions to the Right of Subject Access**

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The School will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after

redaction it is still obvious who the data relates to) then the School do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

**Other Exemptions to the Right of Subject Access**

In certain circumstances the School may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

*Crime detection and prevention*: The School do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

*Confidential references*: The School do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the School receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that the School must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

*Legal professional privilege*: The School do not have to disclose any personal data which is subject to legal professional privilege.

*Management forecasting*: The School do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

*Negotiations*: The School do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

**Refusing to Respond to a Request**

The school can refuse to comply with a request if the request in certain circumstances. These include:

- Where the SAR is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature;
- To avoid obstructing an official or legal inquiry, investigation or procedure;
- To avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- To protect public security;
- To protect national security;
- To protect the rights and freedoms of others.

In the event that you have concerns about supplying the information, you must always refer the matter to the Director of Finance and Operations who will make the decision on our behalf.

In the event that we decide not to comply with the SAR, then the data subject must be informed, without undue delay (and in all cases within one month of receipt of the request), of:

- The reasons we are not taking action;
- That they have a right to make a complaint to the ICO or another supervisory authority; and
- That they are entitled to seek to enforce their right through a judicial remedy.

If a request is found to be manifestly unfounded or excessive the school can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the school need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The school do not need to comply with the request until the fee has been received.

**Record Keeping**

A record of all subject access requests shall be kept by the Director of Finance and Operations. The record shall include the date the SAR was received, the name of the requester, what data the School sent to the requester and the date of the response.

## Appendix 2 – Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

### Proof of Identity

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

### Section 1

Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

| | |
|---|---|
| Title | |
| Surname/Family Name | |
| First Name(s)/ Forename | |
| Date of Birth | |
| Address | |
| Post Code | |
| Phone Number | |
| Email address | |

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

Personal Information

*If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.*

Details:

Employment records:

If you are, or have been employed by the School and are seeking personal information in relation to your employment please provide details of your staff number, unit, team, dates of employment etc.

Details:

**Section 2**

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

| | |
|---|---|
| Title | |
| Surname/ Family Name | |
| First Name(s)/Forenames | |
| Date of Birth | |
| Address | |
| Post Code | |
| Phone Number | |

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

**What is your relationship to the data subject?** (e.g., parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

- ☐ Letter of authority
- ☐ Lasting or Enduring Power of Attorney
- ☐ Evidence of parental responsibility

- Other (give details):

**Section 3**

Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:

- Receive the information by post*
- Receive the information by email
- Collect the information in person
- View a copy of the information only
- Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to: office@oakwoodschool.uk

**APPENDIX 3**

## Data Breach Policy

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The UK GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the School of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

## Definitions

| | |
|---|---|
| **Personal Data** | Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.<br><br>Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.<br><br>Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual. |

| | |
|---|---|
| **Special Category Data** | Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions |
| **Personal Data Breach** | A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data or special category data transmitted, stored or otherwise processed. |
| **Data Subject** | Person to whom the personal data relates. |
| **ICO** | The ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information. |
| **Data Protection Officer (DPO)** | The person we appoint from time to time to lead the development and implementation of our data protection and compliance with the UK GDPR and other applicable. |

## Responsibility

The Director of Finance and Operations has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

In the absence of the Director of Finance and Operations, please contact the Headteacher.

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed.

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

## Security and Data Related Policies

We must keep personal data secure against loss or misuse. All staff are required to comply with our information security guidelines and policies. In particular, staff should refer to the following policies that are related to this Data Breach Policy: -

- *Security Policy* which sets out the School's guidelines and processes on keeping personal data secure against loss and misuse.

- *Data Protection Policy* which sets out the School's obligations under UK GDPR about how they process personal data.

- *Cyber Security Policy* which sets out the School's obligations and guidelines for cyber security issues.

These policies are also designed to protect personal data and can be found at the Staff Share drive and on the school's website.

## Data Breach Procedure

*What is a personal data breach?*

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored for example, loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example, sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it;
- Alteration of personal data without permission;
- Loss of availability of personal data.

*When does it need to be reported?*

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed, the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- Potential or actual discrimination;
- Potential or actual financial loss;
- Potential or actual loss of confidentiality;
- Risk to physical safety or reputation;
- Exposure to identity theft (for example, through the release of non-public identifiers such as passport details); and
- The exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

## Reporting a Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

- Complete a data breach report form (Appendix 1);
- Email the completed form to the Director of Finance and Operations.

Where appropriate, you should liaise with your line manager about completion of the data report form. However, this may not be appropriate or possible, e.g., if your line manager is aware of the breach and instructed you not to report it, or if they are simply not available. In these circumstances, you should submit the report directly to the Director of Finance and Operations, without consulting your line manager. Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, the Director of Finance and Operations or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The Director of Finance and Operations will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

## Managing and Recording the Breach

On being notified of a suspected personal data breach, the Director of Finance and Operations will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so, they will take steps to:-

- Where possible, contain the data breach and (so far as reasonably practicable) recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO where required;
- Notify data subjects affected by the breach if required;

- Notify other appropriate parties to the breach; and
- Take steps to prevent future breaches.

**Containment and Recovery**

The Director of Finance and Operations with the support of our DPO will identify how the breach occurred and take immediate steps to stop of minimise further loss, destruction or unauthorised disclosure of personal data.

The Director of Finance and Operations with the support of our DPO will identify ways to recover, correct or delete data. This may include contacting the police, e.g., where the breach involves stolen hardware or data.

Depending on the nature of the breach, the Director of Finance and Operations with the support of our DPO, will notify the London Borough of Hilliingdon as the insurer can provide access to data breach management experts.

**Notifying the ICO**

The Director of Finance and Operations will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (i.e., it is not 72 working hours). If the School are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

If the school are unsure whether to report, the presumption should be to report. The school will take into account of the factors set out below:

*The potential harm to the rights and freedoms of data subjects*

This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include:

- Exposure to identify theft through the release of non-public identifiers, e.g. passport number;
- Information about the private aspects of a persons life becoming known to others, e.g. financial circumstances;

*The personal data breach must be reported unless it is unlikely to result in a risk to data subjects' rights and freedoms.*

*The volume of personal data*

There should be a presumption to report to the ICO where:

- A large volume of personal data is concerned; and
- There is a real risk to individuals suffering some harm.

It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances if the loss or the extent of information about each individual.

*The sensitivity of data*

There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.

This is most likely to be the case where the breach involves special category personal data. If the information is particularly sensitive, even a single record could trigger a report. The ICO provides two examples:

- theft of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals would be reportable;
- breach of a similar system holding the trade union subscription records of the same number of individuals (where there are no special circumstances surrounding the loss) would not be reportable.

**Notifying Data Subjects**

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Director of Finance and Operations will notify the affected individuals without undue delay including the name and contact details of the DPO and the ICO, the likely consequences of the data breach and the measures the School have (or intended) to take to address the breach, including where appropriate, recommendations for mitigating potential adverse effects.

When determining whether it is necessary to notify individuals directly of the breach, the Director of Finance and Operations will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example, by making a statement on the School website).

**Notifying the Police**

The School will already have considered whether to contact the police for the purpose of containment and recovery. Regardless of this, if it subsequently transpires that the breach arose from a criminal act, the school will notify the police and/or relevant law enforcement authorities.

## Notifying Other Authorities

The School will need to consider whether other parties need to be notified of the breach. For example:

- The Information Commissioners Office (ICO);
- Affected data subjects;
- Insurers;
- Parents;
- Third parties (for example, when they are also affected by the breach);
- Local authority;
- The police (for example, if the breach involved theft of equipment or data).

This list is non-exhaustive.

## Assessing the Breach

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover, correct or delete data (for example, notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e., the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation, two factor authentication);
- What has happened to the data, e.g., if data has been stolen, could it be used for harmful purposes;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

## Preventing Future Breaches

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it is necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

## Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to the Director of Finance and Operations or the DPO. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

## Staff Awareness and Training

Key to the success of our systems is staff awareness and understanding. We provide regular training to staff:

- At induction;
- When there is any change to the law, regulation or our policy;
- When significant new threats are identified; and
- In the event of an incident affecting our school.

The School will ensure that staff are trained and aware on the need to report data breaches to ensure that they know to detect a data breach and the procedures of reporting them. This policy will be shared with staff.

## Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

## Appendix 1 – Data Breach Report Form

If you know or suspect a personal data breach has occurred, please:

- Complete this form; and
- Email or deliver it to the Director of Finance and Operations and the DPO, ensuring that you mark your email as urgent, with the subject 'Data Breach'.

Time is of the essence with data breaches. You must submit this report as soon as know or suspect there has been a data breach. Do not delay to satisfy yourself whether a data breach has definitely happened and do not contact any individuals who may be affected by the data breach. The Director of Finance and Operations along with DPO, will investigate the potential breach and take necessary actions.

| | |
|---|---|
| Name and contact details of person notifying the actual or suspected breach | *[Insert name and contact details]*<br><br>*If you wish to submit an anonymous report, leave this section blank* |
| Department/manager | *[Insert department from which the report emanated and the relevant manager]* |
| Date of actual or suspected breach | *[Insert date]* |
| Date of discovery of actual or suspected breach | *[Insert date]* |
| Date of this report | *[Insert date]* |
| Summary of the facts | [*Provide as much information as possible – including the amount, sensitivity and type of data involved*] |
| Cause of the actual or suspected breach | *[Provide a detailed account of what happened]* |
| Is the actual or suspected breach ongoing? | Yes ☐<br>No ☐<br>Not known ☐ |
| Who is or could be affected by the actual or suspected breach? | *[Include details of categories and approximate number of data subjects concerned]* |
| Are you aware of any related or other data breaches? | Yes ☐<br>No ☐<br><br>[*If yes, provide more details*] |

**APPENDIX 2**

**Data Retention Policy**

The School has a responsibility to maintain its records and record keeping systems. When doing this, the School will take account of the following factors:

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Accessibility of records and record keeping systems.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the School's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the School from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect. The School may also vary any parts of this procedure, including any time limits, as appropriate in any case.

**Data Protection**

This policy sets out how long employment-related and pupil data will normally be held by the School and when that information will be confidentially destroyed in compliance with the terms of the UK General Data Protection Regulation (UK GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the School. The School's Data Protection Policy outlines its duties and obligations under the UK GDPR.

**Retention Schedule**

Information (hard copy and electronic) will be retained for at least the period specified in the attached retention schedule. When managing records, the School will adhere to the standard retention times listed within that schedule.

The retention schedule refers to all records regardless of the media (e.g., paper, electronic, microfilm, photographic etc) in/on which they are stored. All records will be regularly monitored by the Director of Finance and Operations.

**Destruction of Records**

The schedule is a relatively lengthy document listing the many types of records used by the School and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

Where records have been identified for destruction, they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing personal information or sensitive policy information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate wastepaper merchant. All electronic information will be deleted.

The School maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list the following: -

- File reference (or other unique identifier);
- File title/description;
- Number of files;
- Name of the authorising officer;
- Date destroyed or deleted from system; and
- Person(s) who undertook destruction.

**Retention of Safeguarding Records**

Any allegations made that are found to be malicious must not be part of the personnel records.

For any other allegations made, the School must keep a comprehensive summary of the allegation made, details of how the investigation was looked into and resolved and any decisions reached. This should be kept on the personnel files of the accused.

Any allegations made of sexual abuse should be preserved by the School for the term of an inquiry by the Independent Inquiry into Child Sexual Abuse.. All other records (for example, the personnel file of the accused) should be retained until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer. In 2022 the Independent Inquiry into Child Sexual Abuse (IICSA) concluded and published their final report, leaving a recommendation that all records relating to child sexual abuse should be retained for a period of 75 years.

The ICO has not currently produced guidance or frameworks regarding retention as recommended by the inquiry. Until this has been produced, records will still be retained for a prolonged period as recommended initially by IISCA in order to fulfill potential legal duties that a school may have in relation to the inquiry or any further guidance.

**Archiving**

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by the Director of Finance and Operations. The appropriate staff member, when archiving documents should record in this list the following information: -

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

**Transferring Information to Other Media**

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

## Transferring Information to Another School

If we are a pupil's final school of compulsory education, we will retain the pupil record for the full retention period as specified in this policy. However, if a pupil transfers to another school before completion of their compulsory education. the file should be sent to their next school. The responsibility for retention then shifts onto the next school. We retain the file for a year following transfer in case any issues arise as a result of the transfer.

We may delay destruction for a further period where there are special factors such as potential litigation.

## Responsibility and Monitoring

The Director of Finance and Operations has primary and day-to-day responsibility for implementing this policy. The Data Protection Officer, in conjunction with the School is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The Data Protection Officer will consider the suitability and adequacy of this policy and report improvements directly to management.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this policy and are given adequate and regular training on it.

## Emails

Emails accounts are not a case management tool in itself. Generally, emails may need to fall under different retention periods (for example, an email regarding a health and safety report will be subject to a different time frame to an email which forms part of a pupil record). It is important to note that the retention period will depend on the content of the email and it is important that staff file those emails in the relevant areas to avoid the data becoming lost.

**Pupil Records**

All schools with the exception of independent schools, are under a duty to maintain a pupil record for each pupil. If a child changes schools, the responsibility for maintaining the pupil record moves to the next school. We retain the file for a year following transfer in case any issues arise as a result of the transfer.

**Retention Schedule**

| FILE DESCRIPTION | RETENTION PERIOD |
|---|---|
| **Employment Records** | |
| Job applications and interview records of unsuccessful candidates | Six months after notifying unsuccessful candidates, unless the school has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained |
| Job applications and interview records of successful candidates | Added to staff personnel file and retained in line with that record (6 years after employment ceases) |
| Written particulars of employment, contracts of employment and changes to terms and conditions | Added to staff personnel file and retained in line with that record 6 years after employment ceases. |
| Right to work documentation including identification documents and immigration checks | Kept separately from personnel file and retained for 2 years after employment ceases. **Employer's guide to right to work checks: 21 June 2024** |
| DBS checks and disclosures of criminal records forms | DBS certificates should be destroyed as soon as practicable after the check has been completed and the outcome recorded (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for no longer than 6 months |

| | |
|---|---|
| Change of personal details notifications | No longer than 6 months after receiving this notification |
| Emergency contact details | Destroyed on termination |
| Personnel records | While employment continues and up to six years after employment ceases (Limitation Act 1980) |
| Annual leave records | Six years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year |
| Consents for the processing of personal and sensitive data | For as long as the data is being processed and up to 6 years afterwards |
| Working Time Regulations:<br>• Opt out forms<br>• Records of compliance with WTR | • Two years from the date on which they were entered into<br>• Two years after the relevant period |
| Disciplinary records | 6 years after employment ceases (Limitation Act 1980) |
| Grievance records | 6 years after employment ceases (Limitation Act 1980) |
| Training | 6 years after employment ceases (Limitation Act 1980) or length of time required by the professional body |
| Staff training where it relates to safeguarding or other child related training | Date of the training plus 40 years (This retention period reflects that the IICSA may wish to see training records as part of an investigation) |
| Annual appraisal/assessment records | Current year plus 3 years |
| Professional Development Plans | Life of the plan or plan superseded + 6 years |
| Allegations of a child protection nature against a member of staff including where the allegation is unfounded | 10 years from the date of the allegation or the person's normal retirement age |

| | |
|---|---|
| | (whichever is longer). This should be kept under review.<br>Malicious allegations should be removed. |
| **Financial and Payroll Records** | |
| Pension records | 12 years |
| Retirement benefits schemes – notifiable events (for example, relating to incapacity) | 6 years from the end of the scheme year in which the event took place |
| Payroll and wage records | 6 years after end of tax year they relate to (Taxes Management Act 1970; Income and Corporation Taxes 1988) |
| Maternity/Adoption/Paternity Leave records | 3 years after end of tax year they relate to (Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)) |
| Statutory Sick Pay | 3 years after the end of the tax year they relate to (Taxes Management Act 1970; Income and Corporation Taxes 1988) |
| Current bank details | Until updated plus 3 years (Taxes Management Act 1970; Income and Corporation Taxes 1988) |
| Bonus Sheets | Current year plus 3 years (Taxes Management Act 1970; Income and Corporation Taxes 1988) |
| Time sheets/clock cards/flexitime | Current year plus 3 years (Taxes Management Act 1970; Income and Corporation Taxes 1988) |
| Pupil Premium Fund records | Date pupil leaves the provision plus 6 years |

| | |
|---|---|
| National Insurance (schedule of payments) | Current year plus 6 years (Taxes Management Act 1970; Income and Corporation Taxes 1988) |
| Insurance | Current year plus 6 years (Taxes Management Act 1970; Income and Corporation Taxes 1988) |
| Overtime | Current year plus 3 years (Taxes Management Act 1970; Income and Corporation Taxes 1988) |
| Annual accounts | Current year plus 6 years |
| Loans and grants managed by the School | Date of last payment on loan + 6 years if the loan is under 10,000 or date of last payment on loan + 12 years if the loan is over 10,000 |
| All records relating to the creation and management of budgets | Life of the budget plus 3 years |
| Invoices, receipts, order books and requisitions, delivery notices | Current financial year plus 6 years |
| Student Grant applications | Current year plus 3 years |
| Pupil Premium Fund records | Date pupil leaves the provision or school plus 6 years |
| School fund documentation (including but not limited to invoices, cheque books, receipts, bank statements etc). | Current year plus 6 years |
| Free school meals registers (where the register is used as a basis for funding) | Current year plus 6 years |
| School meal registers and summary sheets | Current year plus 3 years |
| **Agreements and Administration Paperwork** | |

| | |
|---|---|
| Collective workforce agreements and past agreements that could affect present employees | Permanently |
| Trade union agreements | 10 years after ceasing to be effective |
| Strategic Plan or School Development Plans | Life of plan or until plan superseded + 3 years. If major changes are made to the plan then an archive copy of previous plans should be retained |
| Visitor Signing-in Records | 6 years |
| Newsletters and circulars to staff, parents and pupils | 1 year (and the School may decide to archive one copy) |
| Minutes of Senior Management Team meetings | Date of the meeting plus 3 years or as required |
| Reports created by the Head Teacher or the Senior Management Team. | Date of the report plus a minimum of 3 years or as required |
| Records relating to the creation and publication of the school prospectus | Current academic year plus 3 years |
| **Health and Safety Records** | |
| Health and Safety consultations | Permanently |
| Health and Safety Risk Assessments | Life of the risk assessment plus 3 years |
| Health and Safety Policy Statements | Life of policy plus 3 years |
| Any records relating to any reportable death, injury, disease or dangerous occurrence | Date of incident plus 3 years provided that all records relating to the incident are held on personnel file |
| Accident reporting records relating to individuals who are under 18 years of age at the time of the incident | Until the child reaches the age of 21. (Limitations Act 1980) |
| Accident reporting records relating to individuals who are over 18 years of age at the time of the incident | Date of last entry in the accident book + 3 years but if there is possibility of negligence allegation then date of |

| | |
|---|---|
| | incident + 15 years or date of settlement + 6 years. (Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980) |
| Fire precaution logbooks | Current year plus 6 years |
| Medical records and details of: -<br>• control of lead at work<br>• employees exposed to asbestos dust<br>• records specified by the Control of Substances Hazardous to Health Regulations (COSHH) | 40 years from the date of the last entry made in the record (Control of Substances Hazardous to Health Regulations (COSHH); Control of Asbestos at Work Regulations) |
| Records of tests and examinations of control systems and protection equipment under COSHH | 5 years from the date on which the record was made |
| **Temporary and Casual Workers** | |
| Records relating to hours worked and payments made to workers | 3 years |
| **Governing Body Documents** | |
| Instruments of government | For the life of the School. Consult local archives before disposal |
| Meetings schedule | Current year |
| Minutes – principal set (signed) | Date of meeting + 10 years |
| Agendas – principal copy | Where possible the agenda should be stored with the principal set of the minutes |

| | |
|---|---|
| Agendas – additional copies | Date of meeting |
| Policy documents created and administered by the governing body | Until replaced |
| Register of attendance at full governing board meetings | Date of last meeting in the book plus 6 years |
| Annual Reports created under the requirements of the Education (Governors Annual Reports) (England) (Amendment) Regulations 2002 | Date of report plus 10 years |
| Records relating to complaints made to and investigated by the governing body or head teacher | Major complaints: current year plus 6 years.<br>If negligence involved: current year plus 15 years.<br>If child protection or safeguarding issues are involved then: current year plus 40years. If the complaint relates to child sexual abuse, then indefinitely. (Based on recommendations left by the IICSA, will be reviewed upon publication of ICO guidance) |
| Correspondence sent and received by the governing body or head teacher | General correspondence should be retained for current year plus 3 years |
| Records relating to the terms of office of serving governors, including evidence of appointment | Date appointment ceases plus 6 years except where there have been allegations concerning children. In this case retain for 25 years. |
| Register of business interests | Date appointment ceases plus 10 years<br>(<br>Companies Act 2006) |
| Records relating to the training required and received by governors | Date appointment ceases plus 6 years |
| Records relating to the appointment of a clerk to the governing body | Date on which clerk appointment ceases plus 6 years |
| Governor personnel files | Date appointment ceases plus 6 years |

| **Pupil Records** | |
|---|---|
| Details of whether admission is successful/unsuccessful | 1 year from the date of admission/non-admission (School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels) |
| Proof of address supplied by parents as part of the admissions process | Current year plus 1 year (School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels) |
| Admissions register | Entries to be preserved for six years from date of entry (Working together to improve school attendance, Section, 36, 2024 Statutory guidance) |
| Pupil Record, including non-child protection safeguarding records. | Primary – Whilst the child attends the School (The Education (Pupil Information) (England) Regulations 2005, The Pupil Information (Wales) Regulations 2011)<br>Secondary – until the child reaches the age of 25 (Limitation Act 1980, Section 2) |
| Attendance Registers | Six years from the date of entry (Working together to improve school attendance, Section 36, 2024 Statutory guidance) |
| Correspondence relating to any absence (authorised or unauthorised) | Current academic year plus 2 years (Education Act 1996, Section 7) |

| | |
|---|---|
| Special Educational Needs files, reviews and Education, Health and Care Plan, including advice and information provided to parents regarding educational needs and accessibility strategy | Primary school - whilst the child attends the school.<br>Secondary - Date of birth of the pupil plus 31 years (Education, Health and Care Plan is valid until the individual reaches the age of 25 years – the retention period adds an additional 6 years from the end of the plan).<br>(Children and Family's Act 2014; Special Educational Needs and Disability Act 2001) |
| Child protection information (to be held in a separate file). | DOB of the child plus 25 years then review. If aspects of the record relate to child sexual abuse, then these records should be retained indefinitely. (Based on recommendations left by the IICSA, will be reviewed upon publication of ICO guidance) |
| Exam results (pupil copy) | This information should be added to the pupil file and retained in line with that record. |
| Examination results (school's copy) | Current year plus 6 years |
| Allegations of sexual abuse | If the complaint relates to child sexual abuse, then indefinitely. (Based on recommendations left by the IICSA, will be reviewed upon publication of ICO guidance) |
| Records relating to any allegation of a child protection nature against a member of staff | Until the accused normal retirement age or 10 years from the date of the allegation (whichever is the longer) |

| | |
|---|---|
| | (Retention period informed by the guidance of KCSIE) |
| Consents relating to school activities as part of UK GDPR compliance (for example, consent to be sent circulars or mailings) | Evidence of consent will be retained whilst the pupil attends the school, or until withdrawn, whichever the shorter. |
| Pupil's work | Where possible, returned to pupil at the end of the academic year (provided the School have their own internal policy to this effect). Otherwise, the work should be retained for the current year plus 1 year |
| Mark books | Current year plus 1 year |
| Schemes of work | Current year plus 1 year |
| Timetable | Current year plus 1 year |
| Class record books | Current year plus 1 year |
| Record of homework set | Current year plus 1 year |
| Photographs of pupils | For the time the child is at the School and for a short while after.<br>Please note select images may also be kept for longer (for example to illustrate history of the school) |
| Parental consent forms for school trips where there has been no major incident | End of the trip or end of the academic year (subject to a risk assessment carried out by the School) |
| Parental permission slips for school trips where there has been a major incident | Date of birth of the pupil involved in the incident plus 25 years. Permission slips for all the pupils on the trip should be retained to demonstrate the rules had been followed for all pupils |
| **Other Records** | |

| | |
|---|---|
| Emails | 1 year |
| CCTV | 30 days |
| Privacy notices | Until replaced plus 6 years |
| Inventories of furniture and equipment | Current year plus 6 years |
| All records relating to the maintenance of the School carried out by contractors or employees of the school | Whilst the building belongs to the school |
| Records relating to the letting of school premises | Current financial year plus 6 years |
| Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations | Current year plus 6 years then review |
| Referral forms | While the referral is current |
| Contact data sheets | Current year then review, if contact is no longer active then destroy |

**APPENDIX 3**

**Electronic Information and Communications Policy**

**Introduction**

The School's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service. However, it also brings with it certain risks, some of which may involve potential legal and financial liabilities for both us and you, e.g:

- inadvertently entering into contracts or commitments on behalf of us;
- introducing viruses into our systems;
- breaching copyright or licensing rights;
- breaching data protection rights;
- breaching confidentiality and security;
- defamation; and/or
- bullying, harassment and discriminatory conduct.

This policy aims to guard against those risks. It is therefore important that all staff read the policy carefully and ensure that they use the internet, email and other communication systems in accordance with it. If you are unsure whether something you are about to do complies with this policy, you should seek advice from your line manager.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff at the School who are required to familiarise themselves and comply with its contents. The School reserves the right to amend its content at any time.

This policy outlines the standards that the School requires all users of these systems to observe, the circumstances in which the School will monitor use of these systems and the action the School will take in respect of any breaches of these standards. We expect our computer and communications systems and equipment to be used in an effective and professional manner and encourage all staff to develop the necessary

skills to achieve this. These systems and equipment are provided by us for the purpose of our business, and to assist staff in carrying out their duties effectively. It is the responsibility of all staff to ensure that these systems and equipment are used for proper business purposes and in a manner that does not compromise us or our staff in any way.

All staff should consider how their reputation and that of the School might be affected by how they communicate and conduct themselves online.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data. Therefore, it is regulated by the UK General Data Protection Regulation (UK GDPR) and all data protection laws and guidance in force.

Staff are referred to the School's Data Protection Policy for further information. The School is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the School's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the School's disciplinary procedure and in serious cases, may be treated as gross misconduct leading to summary dismissal.

The School has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the UK GDPR.

**Scope of the Policy**

This policy applies to all staff, including employees, workers, temporary and agency workers, interns, volunteers and apprentices, governors, trustees, consultants and other contractors who have access to our computer and other communications

systems. It also applies to personal use of our systems and equipment in any way that reasonably allows others to identify any individual as associated us.

This policy applies to the use (or misuse) of computer equipment, e-mail, internet systems, telephones, iPads (and other mobile device tablets), Smart Phones, laptops, Chromebooks, mobile phones and voicemail but it applies equally to the use of fax machines, copiers, scanners, and the like, both in the workplace and from outside (e.g. via remote access).

**Prohibited use and breach of this policy**

We consider this policy to be extremely important. Any breach of the policy will be dealt with under our disciplinary policy. In certain circumstances, breach of this policy may be considered gross misconduct and may result in immediate termination of employment or engagement without notice or payment in lieu of notice. In addition, or as an alternative, we may withdraw an individual's internet and/or email access.

Examples of matters that will usually be treated as gross misconduct include (this list is not exhaustive):

- unauthorised use of the internet;
- creating, transmitting or otherwise publishing any false and defamatory statement about any person or organisation;
- creating, viewing, accessing, transmitting or downloading any material which is discriminatory or may cause embarrassment to other individuals, including material which breaches the principles set out in our equality, diversity and inclusion policies;
- accessing, transmitting or downloading any confidential information about the School and/or any of our staff and/or current, former or prospective pupils or

parents, suppliers, contractors or other such third parties, except where authorised in the proper performance of your duties;

- accessing, transmitting or downloading unauthorised software; and
- viewing, accessing, transmitting or downloading any material in breach of copyright.

**Equipment Security and Passwords**

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Passwords are unique to each user and staff are required to select a password that cannot be easily broken and which contains at least 8 characters including numbers, letters and special characters. All passwords should be considered complex.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with the ICT Network Manager as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If given access to the School e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Team and/or the ICT Network Manager may do spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach

of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off prevents another member of staff or a pupil accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of ICT Network Manager. On the termination of employment for any reason, staff are required to provide a full handover detailing the drives, folders and files where their work can be located and accessed. The School reserves the right to require employees to hand over all School data held in computer useable format.

Members of staff who have been issued with a laptop, iPad (or other mobile device tablet), Smart Phone or any other device (i.e., USB stick) must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the device is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g., ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers. If staff take devices off-site they should follow the Home Working Policy.

**Systems Use and Data Security**

You should not delete, destroy or modify any of the School's existing systems, programs, information or data which could have the effect of harming or exposing to risk of harm the School, its staff, students, or any other party.

You are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the ICT Network Manager who will consider bona fide requests for work purposes. Please note that this includes instant

messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

You must not connect any personal computer, mobile phone, laptop, tablet, USB storage device or other device to our systems or network without express prior permission from the ICT Network Manager. Any permitted equipment must have up-to-date anti-virus software installed on it and we may inspect such equipment in order to verify this

All members of staff need to inform the Director of Finance and Operations before sharing any data with any third parties so the School can carry out a Data Protection Impact Assessment (DPIA).

Where consent is given, all files and data should always be virus checked before they are downloaded onto the School's systems. If in doubt, the employee should seek advice from the ICT Network Manager or a member of the Senior Leadership Team.

The following must never be accessed from the network because of their potential to overload the system or to introduce viruses:

- Audio and video streaming;
- Instant messaging;
- Chat rooms;
- Social networking sites; and
- Web mail (such as Hotmail or Yahoo).

No device or equipment should be attached to our systems without the prior approval of the ICT Network Manager or Senior Leadership Team. This includes but is not limited to, any Smart Phone or telephone, iPad, laptop (or other mobile device tablet), USB device, i-pod, digital camera, infra red connection device or any other device.

The School monitors all e-mails passing through its systems for viruses. Staff should be cautious when opening e-mails from unknown external sources or where for any reason an e-mail appears suspicious (such as ending in '.exe'). The ICT Network Manager should be informed immediately if a suspected virus is received. The School reserves the right to block access to attachments to e-mail for the purpose of effective

use of the system and compliance with this policy. The School also reserves the right not to transmit any e-mail message.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the School's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled Inappropriate Use of the School's Systems and guidance under "E-mail etiquette and content" below.

You must inform the ICT Network Manager immediately if you suspect your computer may have a virus, and you must not use the computer again until informed it is safe to do so.

**E-mail Etiquette and Content**

E-mail is a vital business tool but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.

The School's e-mail facility is intended to promote effective communication within the business on matters relating to the School's business activities and access to the School's e-mail facility is provided for work purposes only.

Staff are permitted to make reasonable personal use of the School's e-mail facility provided such use is in strict accordance with this policy (see Personal Use below). Excessive or inappropriate personal use of the School's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

Staff should always consider if e-mail is the appropriate medium for a particular communication. The School encourages all members of staff to make direct contact with individuals rather than communicate by e-mail wherever possible to maintain and enhance good working relationships.

Messages sent on the e-mail system should be written as professionally as a letter or fax message and should be concise and directed only to relevant individuals on a need to know basis. The content and language used in the message must be consistent with the School's best practice.

Staff must not send messages from another person's email address (unless authorised in the proper performance of their duties), or under an assumed name.

E-mails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to write a draft e-mail first, print it out and review it carefully before finalising and sending. As a rule of thumb if a member of staff would not be happy for the e-mail to be read out in public or subjected to scrutiny then it should not be sent. Hard copies of e-mails should be retained on the appropriate file.

Staff should check the recipient(s) before pressing the send button—not only can it be embarrassing if a message is sent to the wrong person, it can also result in the unintentional disclosure of confidential information and amount to a breach of data protection.

All members of staff should remember that e-mails can be the subject of legal action for example, in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the School. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the School in the same way as the contents of letters or faxes.

E-mail messages may of course be disclosed in legal proceedings in the same way as paper documents. They may also be disclosed as part of dealing with subject access requests when they arise. Deletion from a user's inbox or archives does not mean that an e-mail is obliterated and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

Staff should assume that e-mail messages may be read by others and not include in them anything which would offend or embarrass any reader or themselves, if it found its way into the public domain. The School standard disclaimer should always be used on every e-mail.

Staff should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to e-mails marked 'high priority' as soon as is reasonably practicable.

Members of staff are strictly forbidden from sending or posting messages or material that is offensive, abusive, obscene, discriminatory, racist, sexually suggestive, harassing, derogatory or defamatory messages or which otherwise: -

- May be inconsistent with our equality, diversity inclusion and anti harassment and bullying policies;
- criticise other schools or their staff; or
- state that anyone is incompetent.

This list is not exhaustive.

If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Team immediately. If a recipient asks you to stop sending them personal messages then always stop immediately. Where appropriate, the sender of the e-mail should be referred to this policy and asked to stop sending such material.

If you feel that you have been harassed, bullied or victimized or are offended by material sent to you by a colleague via e-mail, or that you have witnessed, you should inform the Headteacher who will usually seek to resolve the matter informally. You should refer to our Equal Opportunities and Diversity Policy and the Anti-Harassment and Bullying Policy for further information and guidance. We encourage staff to report such concerns.

If an informal procedure is unsuccessful, you may pursue the matter formally under the School's formal grievance procedure. (Further information is contained in the School's Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy and Grievance Policy and Procedure.)

**General Guidance**

Staff must not:

- Send any e-mail, including resending and forwarding, containing sexually explicit, suggestive or otherwise offensive material either internally or externally;
- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice;
- Send or forward private e-mails at work which they would not want a third party to read;
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the School;
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- Sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals.
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;
- Download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- Send messages containing any reference to other individuals or any other business that may be construed as libellous;

- Send messages from another worker's computer or under an assumed name unless specifically authorised;
- Send confidential messages via e-mail, the internet or by other means of external communication which are known not to be secure;
- E-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service related issues. Urgent or important messages to family and friends are permitted but must be of a serious nature;

The School recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once and not forward it to any internal or external recipient, other than internally to the data protection officer in order to report a breach of this or another policy. If you believe you may have been bullied, harassed, sexually harassed or victimised, we encourage you to report this. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated.

Staff who receive an e-mail which has been wrongly delivered should return it to the sender of the message and delete the email as soon as possible to minimise any further risk to individuals whose data could be breached. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of staff or used in any way. The Headteacher should be informed as soon as reasonably practicable.

**Emails—monitoring**

We may monitor the email and instant messaging systems or network in the workplace for the following reasons:

1. to determine whether they are communications relevant to the carrying on of our relevant activities;
2. if the individual is absent from work, to check communications for business calls to ensure the smooth running of the School;
3. to record transactions;
4. where we suspect that the individual is sending or receiving messages that are:
    a. detrimental to us;
    b. in breach of the individual's contract, or this policy;
    c. in breach of data protection rights;
    d. to monitor staff conduct;
    e. to investigate complaints, grievances or criminal offences.

When monitoring incoming or outgoing emails, we will, unless exceptional circumstances apply:

1. look at the sender or recipient of the email and the subject heading only; and
2. avoid opening emails marked 'Private' or 'Personal'.

We do not, as a matter of policy routinely monitor employees' use of the internet or the content of email messages sent or received. However, we have a right to protect the security of its systems or network, check that use of the system is legitimate, investigate suspected wrongful acts and otherwise comply with legal obligations imposed upon it. To achieve these objectives, we carry out random spot checks on

the system which may include accessing individual email messages or checking on specific internet sites searched for and/or accessed by individuals.

We will only intercept (i.e. open) outgoing or incoming emails, received emails, sent emails and draft emails where relevant to the carrying on of our business and where necessary:

- to determine whether the message is relevant to the carrying on of our business;
- to establish the existence of facts;
- to check whether regulatory or self-regulatory practices or procedures to which we or our staff are subject have been complied with, i.e. to detect unauthorised use of the system;
- to check whether staff using the system in the course of their duties are achieving the standards required of them;
- for the purpose of investigating or detecting the unauthorised use of the system;
- for the purpose of preventing or detecting crime; or
- for the effective operation of the telecommunication system.

The content of emails will be examined only in exceptional circumstances, initially by the Headteacher. The information obtained through monitoring may be shared internally, if access to the information is necessary for the performance of their roles. Information will usually only be shared in this way where the School believes there may have been a breach of the individual's contract or this Policy.

**Use of the Internet**

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the School, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if for example, the material is pornographic in nature.

Staff must not access any web page or any files from the School's system (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the School (whether intending to view the page or not) might be offended by the contents of a page or if the fact that the School's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Staff should not under any circumstances use School systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time.

Remember also that text, music and other content on the internet are copyright works. Staff should not download or e-mail such content to others unless certain that the owner of such works allows this.

The School's website may be found at https://www.oakwoodschool.uk/. This website is intended to convey our core values and excellence in the educational sector. All members of staff are encouraged to give feedback concerning the site and new ideas and inclusions are welcome. Such input should be submitted to the Senior Leadership Group in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

The School should refrain from texting and using systems such as WhatsApp for School related matters using personal phones. The School require staff to use alternative systems to make contact with staff (such as emails).

The School has published relevant information on its own intranet for the use of all staff. All such information is regarded as confidential to the School and may not be reproduced electronically or otherwise for the purposes of passing it to any individual not directly employed by the School. Any exceptions to this must be authorised by

thee ICT Network Manager who will liaise with the Senior Leadership Team as appropriate and necessary.

**Internet—monitoring**

We may monitor internet usage (including searches made, the IP addresses of sites visited, and the duration and frequency of visits) if we suspect that the individual has been using the internet in breach of the individual's contract or this policy, e.g.:

- by viewing material that is pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and/or which is liable to cause embarrassment to us;
- by spending an excessive amount of time viewing websites that are not work-related.

Monitoring may include internet usage at the workplace, internet usage outside the workplace during working hours using our systems or network and internet usage using hand-held or portable electronic devices.

Monitoring will normally be conducted by our *IT team*. The information obtained through monitoring may be shared internally, if access to the information is necessary for the performance of their roles. Information will usually only be shared in this way where the IT team believes there may have been a breach of the individual's contract or this Policy.

**Personal Use of School Systems**

The School permits the incidental use of its internet, e-mail and telephone systems to send personal e-mail, browse the web and make personal telephone calls subject to certain conditions set out below.

Our policy on personal use is a privilege and not a right. The policy is dependent upon it not being abused or overused and we reserve the right to withdraw our permission or amend the scope of this policy at any time.

The following conditions must be met for personal usage to continue:

(a) Use must be minimal and take place substantially out of normal working hours (that is, during the member of staff's usual break time or shortly, before or after normal working hours);
(b) Personal e-mails must be labelled "personal" in the subject header;
(c) Use must not interfere with business or office commitments;
(d) Use must not commit the School to any marginal costs;
(e) Use must comply at all times with the rules and guidelines set out in this policy;
(f) Use must also comply with the School's compliment of operational policies and procedures including but not limited to the Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy, Data Protection Policy and Code of Conduct.

Staff should be aware that any personal use of the systems may also be monitored (see below) and where breaches of this policy are found, action may be taken under our Disciplinary Policy and Procedure. Any OR Excessive or inappropriate personal use of the School's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

[The School reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers that personal use is excessive or otherwise in breach of this policy.

**Inappropriate Use of Equipment and Systems**

Incidental/occasional/reasonable personal use is permissible provided it is in full compliance with the School's rules, policies and procedures (including this policy, the Equal Opportunities and Diversity Policy, Anti-Harassment Policy, Data Protection Policy, Code of Conduct and Disciplinary Policy and Procedure).

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the School's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing,

accessing, transmitting or downloading any of the following material or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

(a) Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
(b) Transmitting a false and/or defamatory statement about any person or organisation;
(c) Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others;
(d) Transmitting confidential information about the School and any of its staff, students or associated third parties;
(e) Transmitting any other statement which is likely to create any liability (whether criminal or civil and whether for the employee or for the School);
(f) Downloading or disseminating material in breach of copyright;
(g) Copying, downloading, storing or running any software without the express prior authorisation of the ICT Network Manager.
(h) Engaging in online chat rooms, instant messaging, social networking sites and online gambling;
(i) Forwarding electronic chain letters and other materials;
(j) Accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

**APPENDIX 4**

**Freedom of Information Policy and Publication Scheme**

**Introduction**

The Freedom of Information Act 2000 gives individuals the right to access official information from public bodies. Under the Act, any person has a legal right to ask for access to information held by the school. They are entitled to be told whether the school holds the information and to receive a copy, subject to certain exemptions. While the Act assumes openness, it recognises that certain information is sensitive. There are exemptions to protect this information. Full details on how requests can be made are set out in section 1 of this policy.

Public authorities should be clear and proactive about the information they will make public. For this reason, a publication scheme is available and can be found at section 2 of this policy.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect.

This policy should be used in conjunction with the School's Data Protection Policy.

**Section 1 – Freedom of Information Requests**

Requests under Freedom of Information should be made to the Director of Finance and Operations. However, the request can be addressed to anyone in the School. All staff need to be aware of the process for dealing with requests. If staff receive a FOI request in their inbox, it should be instantly forwarded to the Director of Finance and Operations.

Requests for information that are not data protection or environmental information requests will be covered by the Freedom of Information Act.

*Data protection enquiries (or Subject Access Requests/SARs)* are requests where the enquirer asks to see what personal information the school holds about the enquirer. If

the enquiry is a data protection request, the School's Data Protection Policy should be followed.

*Environmental Information Regulations* enquiries are those which relate to air, water, land, natural sites, built environment, flora and fauna, health and any decisions and activities affecting any of these. These could, therefore, include enquiries about recycling, phone masts, school playing fields, car parking etc. If the enquiry is about environmental information, follow the guidance on the Department for Environment, Food and Rural Affairs (DEFRA) website.

Freedom of Information requests *must* be made in writing (including email) and should include the enquirer's name, correspondence address (email addresses are allowed) and state what information they require. There must be enough information in the request to be able to identify and locate the information. If this information is covered by one of the other pieces of legislation (as referred to above), they will be dealt with under the relevant policy/procedure related to that request.

If the request is ambiguous and/or the School require further information in order to deal with your request, the School will request this further information directly from the individual making the request. Please note that the School do not have to deal with the request until the further information is received. Therefore, the time limit starts from the date that the School receives all information required in order to deal with the request.

The requester does not have to mention the Act, nor do they have to say why they want the information. There is a duty to respond to all requests, telling the enquirer whether or not the information is held and supplying any information that is held, except where exemptions apply. There is a time limit of 20 school days (i.e., excluding school holidays) for responding to the request.

**Information**

Provided all requirements are met for a valid request to be made, the School will provide the information that it holds (unless an exemption applies).

Holding information means information relating to the business of the school:

- That the school has created; or
- That the school has received from another body or person; or
- Held by another body on the school's behalf.

Information means both hard copy and digital information, including email.

If the information is held by another public authority (for example, the Local Authority), check whether they hold the information and if so, transfer the request to them. If this applies, the School will notify the enquirer that they do not hold the information and to whom they have transferred the request. The School will continue to answer any parts of the enquiry in respect of information it does hold.

When the School does not hold the information, it has *no duty to create or acquire it* just to answer the enquiry; although a reasonable search will be made before confirming whether the School has the information requested.

If the information requested is already in the public domain, for instance, through the Publication Scheme or on the School's website, the School will direct the enquirer to the information and explain how to access it.

The requester has the right to be told if the information requested is held by the School (subject to any of the exemptions). This obligation is known as the school's *duty to confirm or deny* that it holds the information. However, the school does not have to confirm or deny if:

- The exemption is an absolute exemption; or
- In the case of qualified exemptions, confirming or denying would itself disclose exempted information.

**Vexatious Requests**

There is no obligation on the School to comply with vexatious requests. A vexatious request is one which is designed to cause inconvenience, harassment or expense rather than to obtain information and would require a substantial diversion of resources or would otherwise undermine the work of the school. However, this does not provide an excuse for bad records management.

In addition, the School do not have to comply with repeated identical or substantially similar requests from the same applicant unless a reasonable interval has elapsed between requests.

**Fees**

The School may charge the requester a fee for providing the requested information. This will be dependent on whether the staffing costs in complying with the request exceeds the threshold. The threshold is currently £450 with staff costs calculated at a fixed rate of £25 per hour (therefore 18 hours' work is required before the threshold is reached).

If a request would cost less than the threshold, then the school can only charge for the cost of informing the applicant whether the information is held and communicating the information to the applicant (e.g., photocopying, printing and postage costs).

When calculating costs/threshold, the School can take account of the staff costs/time in determining whether the information is held by the School, locating and retrieving the information and extracting the information from other documents. The School will not take account of the costs involved with considering whether information is exempt under the Act.

If a request would cost more than the appropriate limit (£450), the school can turn the request down, answer and charge a fee or answer and waive the fee.

If the School are going to charge they will send the enquirer a fees notice. The School do not have to comply with the request until the fee has been paid. More details on fees can be found on the Information Commissioner's Office (ICO) website.

If planning to turn down a request for cost reasons or charge a high fee, you should contact the applicant in advance to discuss whether they would prefer the scope of the request to be modified so that, for example, it would cost less than the appropriate limit.

Where two or more requests are made to the School by different people who appear to be acting together or as part of a campaign, the estimated cost of complying with

any of the requests may be taken to be the estimated total cost of complying with them all.

**Time Limits**

Compliance with a request must be prompt and within the time limit of 20 school days (this does not include the school holidays or weekends) or 60 working days if this is shorter. 'School' days is defined by the ICO as any day on which there is a session and the pupils are in attendance. Failure to comply could result in a complaint by the requester to the ICO. The response time starts counting as the first day from the next working day after the request is received (so if a request was received on Monday 6th October the time limit would start from the next working day, the 7th October).Where the School has asked the enquirer for more information to enable it to answer, the 20 school days start time begins when this further information has been received.

If some information is exempt this will be detailed in the School's response.

If a qualified exemption applies and the School need more time to consider the public interest test, the School will reply in 20 school days stating that an exemption applies but include an estimate of the date by which a decision on the public interest test will be made. This should be within a "reasonable" time.

Where the School has notified the enquirer that a charge is to be made, the time period stops until payment is received.

**Third Party Data**

Consultation of third parties may be required if their interests could be affected by release of the information requested and any such consultation may influence the decision.

Consultation will be necessary where:

- Disclosure of information may affect the legal rights of a third party, such as the right to have certain information treated in confidence or rights under Article 8 of the European Convention on Human Rights;
- The views of the third party may assist the School to determine if information is exempt from disclosure; or
- The views of the third party may assist the School to determine the public interest test.

Personal information requested by third parties is also exempt under this policy where release of that information would breach the Data Protection Act. If a request is made for a document (e.g., Governing Body minutes) which contains personal information whose release to a third party would breach the Data Protection Act, the document may be issued by blanking out the relevant personal information as set out in the redaction procedure.

**Exemptions**

The presumption of the Freedom of Information Act is that the School will disclose information unless the Act provides a specific reason to withhold it. The Act recognises the need to preserve confidentiality and protect sensitive material in certain circumstances.

The School may refuse all/part of a request, if one of the following applies: -

1) There is an exemption to disclosure within the Act;
2) The information sought is not held;
3) The request is considered vexatious or repeated; or
4) The cost of compliance exceeds the threshold.

A series of exemptions are set out in the Act which allow the withholding of information in relation to an enquiry. Some are specialised in their application (such as national security) and would not usually be relevant to schools.

There are two general categories of exemptions:-

1) *Absolute*: where there is no requirement to confirm or deny that the information is held, disclose the information or consider the public interest; and
2) *Qualified*: where, even if an exemption applies, there is a duty to consider the public interest in disclosing information.

**Absolute Exemptions**

There are eight absolute exemptions set out in the Act. However, the following are the only absolute exemptions which will apply to the School: -

- Information accessible to the enquirer by other means (for example, by way of the School's Publication Scheme);
- National Security/Court Records;
- Personal information (i.e., information which would be covered by the Data Protection Act);
- Information provided in confidence.

If an absolute exemption exists, it means that disclosure is not required by the Act. However, a decision could be taken to ignore the exemption and release the information taking into account all the facts of the case if it is felt necessary to do so.

**Qualified Exemptions**

If one of the below exemptions apply (i.e., a qualified disclosure), there is also a duty to consider the public interest in confirming or denying that the information exists and in disclosing information.

The qualified exemptions under the Act which would be applicable to the School are: -

- Information requested is intended for future publication (and it is reasonable in all the circumstances for the requester to wait until such time that the information is actually published);

- Reasons of national security;
- Government/international relations;
- Release of the information is likely to prejudice any actual or potential legal action or formal investigation involving the School;
- Law enforcement (i.e., if disclosure would prejudice the prevention or detection of crime, the prosecution of offenders or the administration of justice);
- Release of the information would prejudice the ability of the School to carry out an effective audit of its accounts, resources and functions;
- For health and safety purposes;
- Information requested is environmental information;
- Information requested is subject to legal professional privilege; and
- For *commercial interest* reasons.

Where the potential exemption is a qualified exemption, the School will consider the public interest test to identify if the public interest in applying the exemption outweighs the public interest in disclosing it.

In all cases, before writing to the enquirer, the person given responsibility by the School for dealing with the request will need to ensure that the case has been properly considered and that the reasons for refusal or public interest test refusal, are sound.

**Refusal**

If it is decided to refuse a request, the School will send a refusals notice, which must contain:

- The fact that the responsible person cannot provide the information asked for;
- Which exemption(s) apply;
- Why the exemption(s) apply to this enquiry (if it is not self-evident);
- Reasons for refusal; and
- The School's complaints procedure.

For monitoring purposes and in case of an appeal against a decision not to release the information or an investigation by the Information Commissioner, the responsible person must keep a record of all enquiries where all or part of the requested information is withheld and exemptions are claimed. The record must include the reasons for the decision to withhold the information.

The School will get advice from their Data Protection Officer (DPO) prior to withholding data under an exemption or refusing the request in its entirety.

## Section 2 – Freedom of Information Publication Scheme

This publication scheme follows a model approved by the Information Commissioners Office.

This scheme is not a list of individual publications but rather a description of the classes of types of information that we are committed to publishing. This list is not an exhaustive list of all of the types of information that we publish. We try to proactively publish as much information as we can where the information would have a wider public interest.

This scheme does not include information that we consider to be sensitive, such as personal information, information prevented from disclosure by law or information about security matters.

## Classes of Information

There are six classes of information that we hold:

- Who we are and what we do
- What we spend and how we spend it
- What our priorities are and how we are doing
- How we make decisions
- Our policies and procedures
- The services we offer

## Making Information Available

Information will generally be made available on the school website. Where it is not possible to include this information on the school website, or when an individual does not wish to access the information by the website the school will indicate how information can be obtained by other means and provide it by those means. This may be detailed in response to a request or within the scheme itself. This will usually be by way of a paper copy.

In some exceptional circumstances, some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where we are legally required to translate any information, we shall do so.

**Charges for Information Published Under This Scheme**

The school may charge individuals for information published under this scheme. The purpose of this scheme is to make the maximum amount of information readily available at the minimum inconvenience and cost to the public. Charges made by the school for routinely published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on the website will be provided free of charge.

Charges may be made for information subject to a charging regime specified by law.

Charges will be made to cover:

- Photocopying;
- Postage and packaging; and
- The costs directly incurred as a result of viewing information.

Single copies of information requested which are covered by the publication scheme will be provided free unless otherwise stated within the scheme. If the request involved a large amount of photocopying, printing or postage, then this may be at a cost. If this is the case we will let you know as well as let you know the cost before fulfilling your request.

**How to Request Information**

If you require a paper version of any of the documents within the scheme, please contact the school using the contact details below.

Telephone: 01895 237350

Email: office@oakwoodschool.uk

Address: Oak Wood School, Sutton Court Road, Hillingdon, Uxbridge UB10 9HT

Please mark all correspondence *Publication Scheme Request* in order to help us process your request quickly. If the information you are looking for isn't available via the scheme, you can still contact the school to ask if we have this information.

**The Publication Scheme**

| **Who We Are and What We Do** | **Description** |
|---|---|
| Information relating to the Governing Body | Information contained in official governing body documents including the governor's annual report:-<br>• Who is who<br>• Basis of governors appointment<br>• The manner in which the governing body is constituted<br>• Category of the school<br>• A statement on progress in implementing the action plan drawn up following an inspection<br>• Agreed minutes from governors board and committee meetings<br>• A financial statement – including gifts made to the school and amounts paid to the governors for expenses<br>• Information about the implementation of the governing body's policy on pupils with special educational needs and any changes to the policy during the last year<br>• A description of arrangements for the admission of pupils with disabilities, including details of the steps to prevent disabled students being treated less favourably than other pupils, details of existing facilities to assist access to the school by pupils with disabilities, the accessibility plan |

| | |
|---|---|
| | covering future policies for increasing access by those with disabilities to the school<br>• A statement of policy on whole staff development identifying how teacher's professional development impacts on teaching and learning.<br>• Number of pupils on roll and rates of pupils authorised and unauthorised absence<br>• National curriculum assessment results for appropriate key stages with national summary figures<br>• Instruments of government, including the date it takes effect<br>• The term of office of each category of governor if it lasts less than 4 years and the name of anybody entitled to appoint any category of governor. |
| School prospectus | • The name, address, website and telephone number of the school and the type of school<br>• The name of the school Headteacher<br>• The school's staffing structure<br>• Information about the schools policy on providing for pupils with special educational needs<br>• Statement on the schools aims and values<br>• Information on the school policy on admissions<br>• School term dates, times and attendance<br>• Uniform<br>• Number of pupils on roll and rates of student absence |

| What We Spend and How We Spend It | Description |
|---|---|
| Financial statement for the current and previous financial year | Relating to projected and actual income and expenditure, procurement, contracts and financial audit. Includes budget plans, financial statements and financial audit reports. |
| Details of expenditure | Sets out details of items of expenditure over £5,000 including the cost, name of supplier and information about the transaction. |
| Procurement and contracts | Details of the procurement and contracts the school has entered into or details relating to the organisation who has carried out this process on the schools behalf (for example the local authority). |
| Pay policy | A copy of the pay policy that the school uses to govern staff pay. |
| Allowances | Details of allowances and expenses that can be incurred by staff and governors. |
| Pupil Premium | How the school uses pupil premium. |
| Utilities and school running expenditure | Details of the school's overheads and running costs. |

| What Our Priorities Are and How We Are Doing | Description |
|---|---|
| Ofsted report | A published report of the outcome of our latest Ofsted inspection. |
| Performance management Policy | Statement of procedures adopted by the governing body relating to the performance management of staff and the |

| | |
|---|---|
| | annual report of the Headteacher on the effectiveness of appraisal procedures. |
| Charging and remissions policies | A statement of the school's policy with respect to charges and remissions for any optional extra or board and lodging for which charges are permitted, for example school publication, music tuition, trips. |
| Health and Safety Policy and Risk Assessment | Statement of general policy with respect to health and safety at work of employees (and others) and the organisation and arrangements for carrying out the policy. |
| Staff Conduct, Discipline and Grievance | Statement of procedure for regulating conduct and discipline of school staff and procedures by which staff may seek redress for grievance. |
| Curriculum circulars and Statutory Instruments | Any statutory instruments, departmental circulars and administrative memoranda sent by the Department of Education to the Headteacher or governing body relating to the curriculum. |

| **How We Make Decisions** | **Description** |
|---|---|
| Admissions Policy/ Decisions (not individual) | This does not include individual decisions. This is a statement of our policy with regards to admissions and how we make decisions regarding admissions. |

| **Our policies and procedures** | **Description** |
|---|---|

| | |
|---|---|
| Home-School Agreement | Written statements of the schools aims and values, the schools responsibilities, the parental responsibilities the schools expectations of its pupils for example homework arrangements. |
| Curriculum Policy | Statement on following the national curriculum subjects, including any syllabus used by the school. |
| Complaints Policy | Statement of procedures for dealing with complaints. |
| Equality and Diversity Policy | Statement on ensuring that the school follows and promotes equality and diversity. |
| Child protection and safeguarding policy | Statement of policy for safeguarding and promoting welfare of pupils at the school. |
| Relationships and Sex Education Policy | Statement of policy with regard to sex and relationship education. |
| Inclusion Policy | Information about the school's policy on providing for pupils with special educational needs. |
| Behaviour Policy | Statement of general principles on behaviour and discipline and of measures taken by the Headteacher to prevent bullying. |

| **The services we offer** | **Description** |
|---|---|
| Extra-curricular activities and out of school clubs | Details of these are contained in our newsletter and on the school website. |

**Internal Review**

The requester has the right to ask for an internal review if they are dissatisfied with the handling of a request.

Internal review requests should be made within 40 working days of the initial response. This deadline should be communicated to the requester in that response. We are not obliged to provide a review if it is requested after more than 40 working days.

Requests for internal review must make clear why they are dissatisfied with the original decision, detailing why they feel that the School has not complied with Freedom of Information Law.

**Complaints and/or Appeals**

Any written (including email) expression of dissatisfaction should be handled through the School's existing complaints policy. Wherever practicable the review should be handled by someone not involved in the original decision.

If the complainant is dissatisfied with the outcome at Stage 1 of the Complaints Policy and wishes to take the matter further, they can escalate the complaint to Stage 2 – a meeting with members of the governing body's complaints committee, which will be formed of three members. This is the final stage of the Complaints Policy.

The school should maintain records of all complaints and their outcome.

**APPENDIX 5**

**Privacy Notice for Pupils and Parents**

This privacy notice describes how we collect and use personal information about pupils, in accordance with the UK General Data Protection Regulation (UK GDPR), section 537A of the Education Act 1996 and section 83 of the Children Act 1989.

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

This notice applies to all pupils and parents.

## Who Collects This Information

Oak Wood School is a "data controller" of personal data and gathers and uses certain information about pupils and parents. This means that we are responsible for deciding how we hold and use personal information about pupils and parents. Under data protection legislation, we are required to notify you of the information contained in this privacy notice.

This notice does not form part of any contract to provide services and we may update this notice at any time.

It is important that you read this notice with any other policies mentioned within this privacy notice, so that you are aware of how and why we are processing your information, what your rights are under data protection legislation and the procedures we take to protect your personal data.

## Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

## Categories of Pupil Information We Collect, Process, Hold and Share

We may collect, store and use the following categories of personal information about you:

- Personal information such as name, pupil number, date of birth, gender and contact information;
- Emergency contact and family lifestyle information such as names, relationship, phone numbers and email addresses;
- Characteristics (such as language, and free school meal eligibility);
- Attendance details (such as sessions attended, number of absences and reasons for absence);
- Performance and assessment information;

- Behavioural information (including exclusions);
- Images of pupils engaging in school activities, and images captured by the School's CCTV system;
- Information about the use of our IT, communications and other systems, and other monitoring information;
- Financial details;
- Post 16 learning information;
- Recordings of pupils and/or parents from the school's video conferencing platform;

We may also collect, store and use the following more sensitive types of personal information:

- Information about your race or ethnicity, religious or philosophical beliefs
- Information about your health, including any medical conditions and sickness records.
- Special educational needs information;
- Biometric data

**How We Collect this Information**

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. To comply with the UK General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

**How and Why We Use Your Personal Information**

We will only use your personal information when the law allows us to do so. Most commonly, we will hold pupil data and use it for:

- Pupil selection (and to confirm the identity of prospective pupils and their parents);
- Providing education services and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;
- Informing decisions such as the funding of schools;
- Assessing performance and to set targets for schools;
- Safeguarding pupils' welfare and providing appropriate pastoral (and where necessary medical) care;
- Support teaching and learning;
- Giving and receive information and references about past, current and prospective pupils, and to provide references to potential employers of past pupils;
- Managing internal policy and procedure;
- Enabling pupils to take part in assessments, to publish the results of examinations and to record pupil achievements;
- To carry out statistical analysis for diversity purposes;

- Legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with legal obligations and duties of care;
- Enabling relevant authorities to monitor the school's performance and to intervene or assist with incidents as appropriate;
- Monitoring use of the school's IT and communications systems in accordance with the school's IT security policy;
- Making use of photographic images of pupils in school publications, on the school website and on social media channels;
- Security purposes, including CCTV; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.
- To provide support to pupils after they leave the school

**The Lawful Bases on which we use this Information**

We will only use your information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Consent: the individual has given clear consent to process their personal data for a specific purpose;
- Contract: the processing is necessary for a contract with the individual;
- Legal obligation: the processing is necessary to comply with the law (not including contractual obligations);
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law; and
- The Education Act 1996: for Departmental Censuses 3 times a year. More information can be found at: https://www.gov.uk/education/data-collection-and-censuses-for-schools.

We need all the categories of information in the list above primarily to allow us to comply with legal obligations. Please note that we may process information without knowledge or consent, where this is required or permitted by law.

**How we use particularly sensitive personal information**

Special categories of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation, or biometrics require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations in line with our data protection policy.

- Where it is needed in the public interest, such as for equal opportunities monitoring.
- Where it is necessary to protect you or another person from harm.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

**Sharing Data**

We may need to share your data with third parties where it is necessary. There are strict controls on who can see your information. We will not share your data if you have advised us that you do not want it shared unless it's the only way we can make sure you stay safe and healthy, or we are legally required to do so.

We share pupil information with:

- the Department for Education (DfE) - on a statutory basis under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013;
- Ofsted;
- Other Schools that pupils have attended/will attend;
- NHS;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- Local Authority Designated Officer;
- Professional advisors such as lawyers and consultants;
- Support services (including insurance, IT support, information security);
- Providers of learning software; and
- The Local Authority.
- Youth support services – under section 507B of the Education Act 1996, to enable them to provide information regarding training and careers as part of the education or training of 13–19-year-olds;

The Department for Education request regular data sharing on pupil attendance to help support those vulnerable students and to assist with intervention strategies. Further information on how the Department for Education collects this data will be made available on the school website.

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

**Biometric Data**

At Oak Wood School we would like to use your information as part of an automated (i.e. electronically operated) recognition system. This is for the purposes of [specify what purpose is – e.g., catering, library access]. The information that we wish to use

is referred to as 'biometric information'. This data will only be processed once we have obtained appropriate consent. For further information in relation to this, please see our Biometrics Policy.

**Retention Periods**

Except as otherwise permitted or required by applicable law or regulation, the school only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

Information about how we retain information can be found in our Data Retention policy. This document can be found as an Appendix to the Data Protection Policy and on our school website.

**Security**

We have put in place measures to protect the security of your information (i.e., against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. The school keep information about pupils on computer systems and sometimes on paper.

You can find further details of our security procedures within our Data Breach policy and our Information Security policy, which can be found as an Appendix to the Data Protection Policy and on our school website.

It is important that the personal information we hold about you is accurate and current. Please keep us information if yours or your child's personal information changes while your child attends our school.

**Youth Support Services**

*Pupils aged 13+*

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13–19-year-olds under section 507B of the Education Act 1996.

We must provide the pupils name, the parents name(s) and any further information relevant to the support services role.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that only their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

*Pupils aged 16+*
We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13–19-year-olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

**The National Pupil Database**

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data?
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's education record, contact the Director of Finance and Operations.

## Your Rights of Access, Correction, Erasure and Restriction

Under certain circumstances, by law you have the right to:

- Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.
- To object to processing in certain circumstances (for example for direct marketing purposes).
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact the Director of Finance and Operations in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

## Right to Withdraw Consent

In circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Director of Financee and Operations. Once we have received notification that you have withdrawn your consent, we will no longer process

your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

## Contact

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with the Director of Fiinance and Operations in the first instance.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by the Director of Finance and Operations, then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues at https://ico.org.uk/concerns.

## Changes to this Privacy Notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

**APPENDIX 6**

**Privacy Notice for Governors and Volunteers**

This privacy notice describes how we collect, store and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

This notice applies to governors and volunteers.

**Who Collects this Information**

Oak Wood School is a "data controller" of personal data and gathers and uses certain information about you. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice with any other policies mentioned within this privacy notice, so that you are aware of how and why we are processing your information, what your rights are under data protection legislation and the procedures we take to protect your personal data.

**Data Protection Principles**

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

**Categories of Information We Collect, Process, Hold and Share**

We may collect, store and use the following categories of personal information about you:

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Emergency contact information such as names, relationship, phone numbers and email addresses;
- Education details;
- DBS details;
- Employment details;
- Information about business and pecuniary interests;
- Information acquired as part of your application to become a governor;

- Criminal records information as required by law to enable you to work with children;
- Information about your use of our IT, communications and other systems, and other monitoring information;
- Photographs;
- Images captured by the School's CCTV system;
- Video recordings capture by the School's video conferencing platform;
- Details in references about you that we give to others.

We may also collect, store and use the following more sensitive types of personal information:

- Information about your race or ethnicity, religious or philosophical beliefs
- Information about your health, including any medical conditions.
- Biometric data

**How We Collect this Information**

The majority of the information that we collect from you is mandatory, however there is some information that you can choose whether or not to provide to us. Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

We may collect this information from you directly, or from a number of third-party sources, such as other governors and volunteers, the DBS, technical networks and so on.

**How and Why We Use Your Information**

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Where you have provided your consent;
- Where we need to perform a contract we have entered into with you;
- Where we need to comply with a legal obligation (such as health and safety legislation and under statutory codes of practice);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.

The situations in which we will process your personal information are listed below: -

- To determine appointment and suitability as a governor;
- To deal with election of governors;
- To comply with safeguarding obligations;
- To provide details on our website or online databases about governors;
- To communicate with third parties and other stakeholders to the School;

- For business management and planning purposes (including accounting, budgetary and health and safety purposes;
- For financial purposes (such as expenses);
- To deal with any complaints/investigations as required;
- When you sit on a panel or committee, name and comments as well as decisions made;
- To send communications in your role as governor;
- For education, training and development requirements;
- In order to review governance of the School;
- In order to comply with any legal dispute or any legal obligations;
- In order to comply with regulatory requirements or health and safety obligations;
- To ensure system security, including preventing unauthorised access to our networks;
- To monitor use of our systems to ensure compliance with our IT processes;
- To receive advice from external advisors and consultants;
- To liaise with regulatory bodies (such as the DfE, DBS); and
- Dealing with termination of your appointment;

If you fail to provide certain information when requested, we may be prevented from complying with our legal obligations (such as to ensure health and safety). Where you have provided us with consent to use your data, you may withdraw this consent at any time.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

**How We Use Particularly Sensitive Information**

Sensitive personal information (as defined under the UK GDPR as “special category data”) requires higher levels of protection and further justification for collecting, storing, and using. We may process this data in the following circumstances: -

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to our pension scheme);
- Where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else’s interests) and you are not capable of giving your consent.

**Criminal Convictions**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations.

Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

**Sharing Data**

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. These include the following:

- Government departments or agencies
- The Local Authority
- Suppliers and Service providers
- Professional advisors and consultants
- The Department for Education
- Law enforcement
- Support services;
- DBS

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

**Retention Periods**

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

Once you are no longer a governor or volunteer of the school we will retain and securely destroy your personal information in accordance with our data retention policy. This can be found as an Appendix to the Data Protection Policy and on our school website.

**Security**

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

You can find further details of our security procedures within our Data Breach policy and our Information Security policy, which can be found as an Appendix to the Data Protection Policy and on our school website.

It is important that you read this notice with any other policies mentioned within this privacy notice, so that you are aware of how and why we are processing your information, what your rights are under data protection legislation and the procedures we take to protect your personal data.

**Biometric Data**

At Oak Wood School we would like to use your information as part of an automated (i.e., electronically operated) recognition system. This is for the purposes of catering, library access. The information that we wish to use is referred to as 'biometric information'. This data will only be processed once we have obtained appropriate consent. For further information in relation to this, please see our Biometrics policy.

**Your Rights of Access, Correction, Erasure and Restriction**

Under certain circumstances, by law you have the right to:

- Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.
- To object to processing in certain circumstances (for example for direct marketing purposes).
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact the Director of Finance and Operations in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

**Right to Withdraw Consent**

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Director of Finance and Operations. Once we have received notification that you have withdrawn your consent, we will no

longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

**How to Raise a Concern**

We hope that the Director of Finance and Operations can resolve any query you raise about our use of your information in the first instance.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by the Director of Financee and Operations, then you can contact the DPO on the details below: -

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

**Changes to this Privacy Notice**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

**APPENDIX 7**

**Privacy Notice for Job Applicants**

This privacy notice describes how we collect and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR

Successful candidates should refer to our privacy notice for staff for information about how their personal data is stored and collected.

**Who Collects this Information**

Oak Wood School is a "data controller" of personal data and gathers and uses certain data about you. This means that we are responsible for deciding how we hold and use personal information about you.

We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice, together with any other policies mentioned within this privacy notice. This will assist you with understanding how we process your information and the procedures we take to protect your personal data.

**Data Protection Principles**

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

**Categories of Information We Collect, Process, Hold and Share**

We may collect, store and use the following categories of personal information about you up to the shortlisting stage of the recruitment process: -

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Emergency contact information such as names, relationship, phone numbers and email addresses;
- Information collected during the recruitment process that we retain during your employment including proof of right to work in the UK, information entered on the application form, CV, qualifications;
- Details of your employment history including job titles, salary and working hours;

- Information regarding your criminal record as required by law to enable you to work with children;
- Details of your referees and references;
- Details collected through any pre-employment checks including online searches for data;
- Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs.

We may also collect information after the shortlisting and interview stage in order to make a final decision on where to recruit:

- Data about your previous academic and/or employment history, including details of any conduct, grievance or performance issues, appraisals, time and attendance, from references obtained about you from previous employers and/or education providers;
- Data regarding your academic and professional qualifications;
- Data regarding your criminal record**,** in a criminal records certificate (CRC) or enhanced criminal records certificate (ECRC) as appropriate**;**
- Your nationality and immigration status and data from related documents, such as your passport or other identification and immigration information;
- A copy of your driving licence; and
- Data relating to your health.

**How We Collect this Information**

We may collect this information from you, your referees, your education provider, by searching online resources, from relevant professional bodies the Home Office and from the DBS.

**How and Why We Use Your Information**

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Where we need to take steps to enter into a contract with you;
- Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.
- Where you have provided your consent for us to process your personal data.

Generally, the purpose of us collecting your data is to enable us to facilitate safe recruitment and determine suitability for the role. We also collect data in order to carry

out equal opportunities monitoring and to ensure appropriate access arrangements are put in place if required.

If you fail to provide certain information when requested, we may not be able to take the steps to enter into a contract with you, or we may be prevented from complying with our legal obligations.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

**How We Use Particularly Sensitive Information**

Sensitive personal information (as defined under the UK GDPR as "special category data") require higher levels of protection and further justification for collecting, storing, and using this type of personal information. We may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to our pension scheme);
- Where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent.

**Criminal Convictions**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

**Sharing Data**

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

These include the following: -

- Academic or regulatory bodies to validate qualifications/experience (for example the teaching agency);
- Referees;
- Other schools;
- HR advisors and professional advisers.

- DBS; and
- Recruitment and supply agencies.
- our Local Authority in order to meet our legal obligations for sharing data with it;

We may also need to share some of the above categories of personal information with other parties, such as HR consultants and professional advisers. Usually, information will be anonymised but this may not always be possible. The recipients of the information will be bound by confidentiality obligations. We may also be required to share some personal information with our regulators or as required to comply with the law.

**Retention Periods**

We keep the personal data that we obtain about you during the recruitment process for no longer than is necessary for the purposes for which it is processed. How long we keep your data will depend on whether your application is successful and you become employed by us, the nature of the data concerned and the purposes for which it is processed.

We will keep recruitment data (including interview notes) for no longer than is reasonable, taking into account the limitation periods for potential claims such as race or sex discrimination (as extended to take account of early conciliation), after which they will be destroyed. If there is a clear business reason for keeping recruitment records for longer than the recruitment period, we may do so but will first consider whether the records can be pseudonymised, and the longer period for which they will be kept.

If your application is successful, we will keep only the recruitment data that is necessary in relation to your employment.

Once we have finished recruitment for the role you applied for, we will then store your information in accordance with our Retention Policy. This can be found as an Appendix to the Data Protection Policy and on our school website.

**Security**

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

You can find further details of our security procedures within our Data Breach policy and our Information Security policy, which can be found as an Appendix to the Data Protection Policy and on our school website.

**Your Rights of Access, Correction, Erasure and Restriction**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances by law you have the right to:

- Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.
- To object to processing in certain circumstances (for example for direct marketing purposes).
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact the Director of Finance and Operations in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

## Right to Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Director of Finance and Operations. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

## How to Raise a Concern

We hope that the Director of Finance and Operations can resolve any query you raise about our use of your information in the first instance.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by the Director of Finance and Operations, then you can contact the DPO on the details below: -

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

**Changes to this Privacy Notice**

We reserve the right to update this Privacy Notice at any time, and we will provide you with a new privacy notice wen we make any substantial changes. We may also notify you in other ways from time to time about the processing of your personal information.

**APPENDIX 8**

**Privacy Notice for Visitors and contractors**

This privacy notice describes how we collect and use personal information about you during and after your visit with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

This notice applies to all current and former visitors and contractors.

## Who Collects this Information

Oak Wood School is a "data controller" of personal data and gathers and uses certain information about you. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice does not form part of a contract to provide services and we may update this notice at any time.

It is important that you read this notice, with any other policies mentioned within this privacy notice, so you understand how we are processing your information and the procedures we take to protect your personal data.

## Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

## Categories of Visitor Information we Collect, Process, Hold and Share

We process data relating to those visiting our school (including contractors). Personal data that we may collect, process, hold and share (where appropriate) about you includes, but is not restricted to:

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Criminal records information as required by law to enable you to work with children e.g. DBS checks;
- Information relating to your visit, e.g. your company or organisations name, arrival and departure time, car number plate;
- Information about any access arrangements you may need;
- Photographs for identification purposes for the duration of your visit;

- CCTV footage captured by the school.

We may also collect, store and use the following more sensitive types of personal information:

- Information about your race or ethnicity, religious or philosophical beliefs
- Information about your health, including any medical conditions.
- Biometric data

**How we Collect this Information**

We may collect this information from you, the Home Office, the DBS, other professionals we may engage (e.g. to advise us generally), our signing in system, automated monitoring of our websites and other technical systems such as our computer networks and connections, CCTV and access control systems, remote access systems, email and instant messaging systems, intranet and internet facilities.

**How we use your Information**

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Where we need to perform the contract we have entered into with you;
- Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.
- When you have provided us with consent to process your personal data.

We need all the categories of information in the list above primarily to allow us to perform our contract with you, with your consent and to enable us to comply with legal obligations.

The situations in which we will process your personal information are listed below:

- Ensure the safe and orderly running of the school;
- To manage our workforce and those deployed on site;
- Personnel management including retention
- In order to manage internal policy and procedure;
- Complying with legal obligations;
- Carry out necessary administration functions to allow visitors and contractors on site;
- To monitor and manage access to our systems and facilities in order to protect our networks and for the purposes of safeguarding;
- To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution;
- To answer questions from insurers in respect of any insurance policies which relate to you;

- Health and safety obligations;
- Prevention and detection of fraud or other criminal offences; and
- To defend the School in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and will explain the legal basis which allows us to do so.

**How we use Particularly Sensitive Information**

Sensitive personal information (as defined under the UK GDPR as "special category data") require higher levels of protection and further justification for collecting, storing and using this type of personal information. We may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring;
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent.

**Criminal Convictions**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

**Sharing Data**

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. These include the following:

- the Department for Education (DfE);
- Ofsted;
- Law enforcement officials such as police, HMRC;

- LADO;
- Professional advisors such as lawyers and consultants;
- Support services (including HR support, insurance, IT support, information security, pensions and payroll);
- The Local Authority; and
- DBS.

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

**Retention Periods**

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

We will retain and securely destroy your personal information in accordance with our data retention policy. This can be found as an Appendix to the Data Protection Policy and on our school website.

**Security**

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

You can find further details of our security procedures within our Data Breach policy and our Information Security policy, which can be found as an Appendix to the Data Protection Policy and on our school website.

**Biometric Data**

At Oak Wood School we would like to use your information as part of an automated (i.e., electronically operated) recognition system. This is for the purposes of catering. The information that we wish to use is referred to as 'biometric information'. This data will only be processed once we have obtained appropriate consent. For further information in relation to this, please see our Biometrics policy.

**Your Rights of Access, Correction, Erasure and Restriction**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

Under certain circumstances by law you have the right to:

- Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively we may refuse to comply with the request in such circumstances.
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.
- To object to processing in certain circumstances (for example for direct marketing purposes).
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact the Director of Finance and Operations in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

**Right to Withdraw Consent**

In the limited circumstances where you may have provided your consent to the collection, processing, and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Director of Finance and Operations. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

**How to Raise a Concern**

We hope that the Director of Finance and Operations can resolve any query you raise about our use of your information in the first instance.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by the Director of Finance and Operations, then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk

Telephone: 0345 548 7000 option 1 then option 1 again

You have the right to make a complaint at any time to the Information Commissioners Office, the UK supervisory authority for data protection issues.

**Changes to this Privacy Notice**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

**APPENDIX 9**

**Privacy Notice for Staff**

This privacy notice describes how we collect and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

This notice applies to all current and former employees, workers and contractors.

## Who Collects this Information

Oak Wood School is a "data controller" of personal data and gathers and uses certain information about you. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice with any other policies mentioned within this privacy notice, so that you are aware of how and why we are processing your information, what your rights are under data protection legislation and the procedures we take to protect your personal data.

## Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

## Categories of Information We Collect, Process, Hold and Share

Depending on your employment status, we may collect, store and use the following categories of personal information about you:

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Emergency contact information such as names, relationship, phone numbers and email addresses;
- Information collected during the recruitment process that we retain during your employment including references, proof of right to work in the UK, application form, CV, qualifications;
- Employment contract information such as start dates, hours worked, post, roles;

- Education and training details;
- Details of salary and benefits including payment details, bank details, payroll records, tax status information, national insurance number, pension and benefits information;
- Details of any dependants;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- Information in your sickness and absence records such as number of absences and reasons(including sensitive personal information regarding your physical and/or mental health);
- Criminal records information as required by law to enable you to work with children;
- Information on grievances raised by or involving you;
- Information on conduct and/or other disciplinary issues involving you;
- Details of your appraisals, performance reviews and capability issues;
- Details of your time and attendance records;
- Information about the use of our IT, communications and other systems, and other monitoring information;
- Details of your use of business-related social media, such as LinkedIn;
- Images of staff captured by the School's CCTV system;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within the School, you will be notified separately if this is to occur); and
- Details in references about you that we give to other;
- Recordings of staff from the School's video conferencing platform

We may also collect, store and use the following more sensitive types of personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation, and political opinions.
- Trade union membership.
- Information about your health, including any medical condition and sickness records, including:
    - where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill health, injury or disability, the records relating to that decision;
    - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; [and]
    - any health information in relation to a claim made under the permanent health insurance scheme; and
    - where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.
- Biometric data
- Information about criminal convictions and offences.

**How We Collect this Information**

We may collect this information from you in your application form, but we will also collect information in a number of different ways. This could be through the Home Office, our pension providers, medical and occupational health professionals we engage with, your trade union, the DBS, consultants and other professionals we may engage, e.g. to advise us generally and/or in relation to any grievance, conduct appraisal or performance review procedure, and even other employees. Information is also collected through CCTV, access control systems and any IT system the school has in place, such as email, communication systems, remote access systems, instant messaging and voicemail.

**How and Why we use your Information**

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Where we need to perform the contract we have entered into with you;
- Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.
- When you have provided us with consent to process your personal data.

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

The situations in which we will process your personal information are listed below:

- To determine recruitment and selection decisions on prospective employees;
- In order to carry out effective performance of the employees contract of employment and to maintain employment records;
- To comply with regulatory requirements and good employment practice;
- To carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements;
- Enable the development of a comprehensive picture of the workforce and how it is deployed and managed;
- To enable management and planning of the workforce, including accounting and auditing;
- Personnel management including retention, sickness and attendance;
- Performance reviews, managing performance and determining performance requirements;
- In order to manage internal policy and procedure;
- Human resources administration including pensions, payroll and benefits;
- To determine qualifications for a particular job or task, including decisions about promotions;
- Evidence for possible disciplinary or grievance processes;
- Complying with legal obligations;
- To monitor and manage staff access to our systems and facilities in order to protect our networks, the personal data of our employees and for the purposes of safeguarding;

- To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution;
- Education, training and development activities;
- To monitor compliance with equal opportunities legislation;
- To answer questions from insurers in respect of any insurance policies which relate to you;
- Determinations about continued employment or engagement;
- Arrangements for the termination of the working relationship;
- Dealing with post-termination arrangements;
- Health and safety obligations;
- Prevention and detection of fraud or other criminal offences; and
- To defend the School in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you, or we may be prevented from complying with our legal obligations.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

**How We Use Particularly Sensitive Information**

Sensitive personal information (as defined under the UK GDPR as "special category data") requires higher levels of protection and further justification for collecting, storing and using. We may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to our pension scheme);
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent.

We will use this information in the following ways:

- Collecting information relating to leave of absence, which may include sickness absence or family related leave;
- To comply with employment and other laws;
- Collecting information about your physical or mental health, or disability status, to ensure your health and welfare in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to manage sickness absence and to administer benefits;

- Collecting information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- To record trade union membership information to pay trade union premiums and to comply with employment law obligations.

**Criminal Convictions**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

**Sharing Data**

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. These include the following:

- the Department for Education (DfE);
- Ofsted;
- Prospective Employers;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- LADO;
- Training providers;
- Professional advisors such as lawyers and consultants;
- Support services (including HR support, insurance, IT support, information security, pensions and payroll);
- The Local Authority;
- Occupational Health;
- DBS;
- Recruitment and supply agencies; and

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations; we require them to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

**Retention Periods**

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

Once you are no longer a staff member at the School, we will retain and securely destroy your personal information in accordance with our data retention policy. This can be found as an Appendix to the Data Protection Policy and on our school website.

**Security**

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

You can find further details of our security procedures within our Data Breach policy and our Information Security policy, which can be found as an Appendix to the Data Protection Policy and on our school website.

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

**Biometric Data**

At [name of school] we would like to use your information as part of an automated (i.e. electronically operated) recognition system. This is for the purposes of [specify what purpose is – e.g., catering, library access]. The information that we wish to use is referred to as 'biometric information'. This data will only be processed once we have obtained appropriate consent. For further information in relation to this, please see our Biometrics Policy.

**Your Rights of Access, Correction, Erasure and Restriction**

Under certain circumstances, by law you have the right to:

- Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.
- To object to processing in certain circumstances (for example for direct marketing purposes).
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact the Director of Finance and Operations in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

## Right to Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Director of Finance and Operations . Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

## How to Raise a Concern

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with the Director of Finance and Operations in the first instance.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by the Director of Finance and Operations, then you can contact the DPO on the details below: -

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

## Changes to this Privacy Notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal

**APPENDIX 10**

**Information Security Policy**

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the School to achieve this, including to:-

- To protect against potential breaches of confidentiality;
- To ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- To support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- To increase awareness and understanding at the School of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they handle.

**Introduction**

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Staff are referred to the Scol's Data Protection Policy, Data Breach Policy and Electronic Information and Communication Systems Policy for further information. These policies are also designed to protect personal data and can be found as an Appendix to the Data Protection Policy and on our school website.

For the avoidance of doubt, the term ‘mobile devices’ used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to laptops, tablets, digital cameras, memory sticks and smartphones.

## Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the School, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

This policy applies to all members of staff including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

All members of staff are required to familiarise themselves with its content and to comply with the provisions contained within it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School’s Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual’s terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

## General Principles

All data stored on our IT Systems are to be classified appropriately (including, but not limited to personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the School’s Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with the Director of Finance and Operations the appropriate security arrangements for the type of information they access in the course of their work.

All data stored within our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired and upgraded by the ICT Network Manager or by such third party/parties as the Director of Finance and Operations may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including but not limited to the security, integrity and confidentiality of that data) lies with the ICT Network Manager unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the Director of Finance and Operations who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

**Physical Security and Procedures**

Paper records and documents containing personal information, sensitive personal information and confidential information shall be positioned in a way to avoid them being viewed by people passing by as far as possible, e.g. through windows. At the end of the working day or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available storage rooms, locked cabinets, and other storage systems with locks shall be used to store paper records when not in use. If you do not feel you have appropriate and/or sufficient storage available to you, you must inform the Director of Finance and Operations as soon as possible.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where

there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Director of Finance and Operations as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The following measures are taken by the School to ensure physical security of the building/s and storage systems:

- The School carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.]
- The School has an intercom system to minimise the risk of unauthorised people from entering the school premises.
- The School close the school gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.
- CCTV Cameras are in use at the School and monitored by the Premises Team.
- Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

**Computers and IT**

The [ICT Network Manager shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements;
b) ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's management and reporting the outcome of such reviews to the School's management;
c) ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations and other relevant rules whether now or in the

future in force, including but not limited to the UK GDPR and the Computer Misuse Act 1990.

Furthermore, the ICT Network Manager shall be responsible for the following:

a) assisting all members of staff in understanding and complying with this policy;
b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
c) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities and any special security requirements;
d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the Data Protection Officer];
e) taking proactive action, where possible, to establish and implement IT security procedures and to raise awareness among members of staff;
f) monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future; and
g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

**Responsibilities – Members of Staff**

All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

You must immediately inform the Director of Finance and Operations of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Data Breach Policy.

Any other technical problems (including but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the ICT Network Manager immediately.

You are not permitted to install any software of your own without the approval of the ICT Network Manager. Any software belonging to you must be approved by the ICT Network Manager and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

Prior to installation of any software onto the IT Systems, you must obtain written permission by the ICT Network Manager. This permission must clearly state which software you may install and onto which computer(s) or device(s) it may be installed.

Prior to any usage of physical media (e.g., USB memory sticks or disks of any kind) for transferring files, you must make sure to have the physical media virus scanned. Approval from ICT Network Manager must be obtained prior to transferring of files using cloud storage systems.

If you detect any virus this must be reported immediately to the ICT Network Manager (this rule shall apply even where the anti-virus software automatically fixes the problem).

**Access Security**

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the School's network. The School also teach individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT

Department. Biometric log-in methods can only be used if approved by the IT Department.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with the ICT Network Manager as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If you forget your password you should notify the ICT Network Manager to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If necessary, you may write down passwords provided that you store them securely (e.g., in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

Computers and other electronical devices with displays and user input devices (e.g., mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this time period or disable the lock.

All mobile devices provided by the School shall be set to lock, sleep or similar after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

**Data Security**

Personal data sent over the School network will be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the ICT Network Manager who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given, all files and data should always be virus checked before they are downloaded onto the School's systems.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi provided that you follow the ICT Network Managers requirements and instructions governing this use. All usage of your own device(s) whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School Policies (including, but not limited to, this policy). The ICT Network Manager may at any time request the immediate disconnection of any such devices without notice.

**Electronic Storage of Data**

All portable data and in particular personal data should be stored on encrypted drives using methods recommended by the ICT Network Manager.

All data stored electronically on physical media and in particular personal data, should be stored securely in a locked box, drawer, cabinet or similar.

You should not store any personal data on any mobile device, whether such device belongs to the School or otherwise without prior written approval of the Director of Finance and Operations. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the School's computer network in order for it to be backed up.

All electronic data must be securely backed up by the end of the each working day and is done by the ICT Network Manager.

**Homeworking**

You should not take confidential or other information home without prior permission of your Line Manager and only do so where satisfied appropriate technical and practical

measures are in place within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that:

a) the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
b) all confidential material that requires disposal is shredded or in the case of electronical material, securely destroyed as soon as any need for its retention has passed.

**Communications, Transfers, Internet and Email Use**

When using the School's IT Systems, you are subject to and must comply with the School's Electronic Information and Communication Systems Policy.

There are restrictions on international transfers of personal data and transfers to international organisations. Staff may only transfer personal data outside the UK or to any international organisation, with the prior written authorisation of the DPO. You should refer to the Schools Data Protection policy for further information on international transfers.

The School work to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to the ICT Network Manager.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the School cannot accept liability for the material accessed or its consequence.

All personal information and in particular sensitive personal information and confidential information should be encrypted before being sent by email or sent by tracked DX (document exchange) or recorded delivery. You may not send such

information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

Postal, DX, fax and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the School.

Personal or confidential information should not be removed from the School without prior permission from your Line Manager except where the removal is temporary and necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

a) not transported in see-through or other un-secured bags or cases;
b) not read in public places (e.g., waiting rooms, cafes, trains, etc.); and
c) not left unattended or in any place where it is at risk (e.g., in car boots, cafes, etc.)

**Reporting Security Breaches**

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Director of Finance and Operations. All members of staff have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the Director of Finance and Operations shall immediately assess the issue, including but not limited to, the level of risk associated with the issue and shall take all steps necessary to respond to the issue.

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Director of Finance and Operations.

Any attempt to resolve an IT security breach by a member of staff must be under the instruction of and with the express permission of the Director of Finance and Operations.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the Director of Finance and Operations.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Data Breach Policy.

## Related Policies

Staff should refer to the following policies that are related to this Information Security Policy: -

- Electronic Information and Communication Systems Policy;
- Data Breach Policy;
- Data Protection Policy