

# Data Protection Policy



Data protection is an important compliance issue for the School. During the course of the School's activities personal data (sometimes sensitive in nature) is collected, stored and processed. The School, as a "data controller", is liable for the actions of its staff in how data is handled. It is therefore an area where everyone has a part to play in ensuring the School complies with legal obligations, whether that personal data handling is sensitive or routine.

This policy sets out to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA2018). The Information Commissioner's Office (ICO) is responsible for enforcing data protection law.

## Executive Summary:

*It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.*

*A good rule of thumb here is to ask yourself questions such as:*

- *Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?*
- *Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?*
- *What would be the consequences of my losing or misdirecting this personal data?*

*Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.*

## 1. Application of this Policy

This policy applies to staff (past, present and prospective), including employees, workers, volunteers, apprentices and Council members (collectively referred to as "staff" for the purposes of this Policy).

Staff should refer to the School's privacy notices and, where appropriate, to other relevant policies including in relation to the use of internet, email and communications, social media, data retention and acceptable use of IT policy, which contain further information regarding the protection of personal information in those contexts.

All staff who handle personal data are obliged to comply with this policy and must read and understand this policy because it gives important information about:

- the data protection principles with which the School must comply;
- data protection obligations;

- what is meant by personal information (or data) and sensitive personal information (or data);
- how data is gathered, used and (ultimately) deleted, whether personal information or sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information gathered used, stored or transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

**Contractors** – This data protection policy represents a set of standards and safeguards that contractors are expected to meet. This policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether acting as "data processors" on the School's behalf (in which case subject to binding contractual terms) or as "data controllers" responsible for handling such personal data in their own right. Where the School shares personal data with a third party – which may range from other schools, universities, parents, appropriate authorities to professional services – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

## 2. Introduction

The School obtains, keeps and uses personal information (also referred to as data) about job applicants and about current and former employees, workers, contractors, volunteers, council members and apprentices for a number of specific lawful purposes, as set out in the School's [Staff Privacy Notice](#).

The School also obtains, keeps and uses personal information about prospective pupils, current pupils, their families, Seniors, Friends of Wycombe Abbey and residents at the School. The detail relating to how it is collected and processed is set out within separate [Privacy Notice for Parents and Pupils](#), [Privacy Notice for Seniors and Friends of Wycombe Abbey](#) and [Privacy Notice for Residents](#).

This policy sets out how the School complies with data protection obligations and seeks to protect personal information relating to stakeholders. Its purpose is also to ensure that everyone understands and complies with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

Those who handle personal data are obliged to comply with this policy when doing so. Breaches of this policy will result in disciplinary action being considered. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches, or near misses, that pose a significant risk to the School or individuals will be considered a serious matter.

The School has appointed the Head of Compliance who acts as data privacy lead undertaking staff training around data protection and privacy compliance. The Head of Compliance is responsible for monitoring compliance with data protection obligations and with School policies.

## 3. Definitions

The following definitions shall apply to this policy:

**"data controller"** means the person or body that determines the purposes and means of the processing of personal data, and who is legally responsible for how the data is used. For example, the School is a data controller. An independent contractor who makes their own such decisions is also, separately likely to be a data controller.

“**data processor**” means the person or organisation that processes (handles) the data on behalf of the data controller. For example, a payroll software provider with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

“**data breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;

“**data subject**” means the individual to whom the personal information relates;

“**personal information**” (sometimes known as personal data) means information relating to a living individual who can be identified (directly or indirectly) from that information, it can include any form of identifier, digital or contextual, including unique ID numbers, initials, nicknames. This definition includes expressions of opinion or intentions towards that individual. Note that personal information will be created almost constantly in the ordinary course of work duties (such as emails, notes of calls, CPOMS/iSAMS records, minutes of meetings);

“**processing**” means virtually anything done with personal information including obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;

“**pseudonymised**” means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;

“**sensitive personal information**” (sometimes known as ‘**special categories of personal data**’ or ‘sensitive personal data’) means personal information about an individual’s race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual’s health, sex life or sexual orientation; and

“**criminal records information**” means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures. There are separate rules for the processing of personal data relating to criminal convictions and offences.

#### 4. Data Protection Principles

GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

- processed **lawfully, fairly** and in a **transparent** manner;
- collected for **specific and explicit purposes** and only for the purposes it was collected;
- **relevant** and **limited** to what is necessary for the purposes it is processed;
- **accurate** and kept **up to date**;
- **kept no longer than is necessary** for the purposes for which it is processed; and
- processed in a manner that ensures **appropriate security** of personal data.

The GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that the School is also able to demonstrate that processing is lawful. This involves, among other things:

- keeping records of all data processing activities, including by way of logs (using the 9nine application) and policies;
- documenting significant decisions and assessments about how personal data is used (including via formal risk assessment documents called Data Protection Impact Assessments - DPIA); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with,

whether or not reported (and to whom), etc.

## 5. Lawful grounds for processing personal information

The GDPR's broader "accountability" principle requires the School to not only process personal data in a fair and legal manner but to be able to demonstrate that the processing is lawful.

Any processing activity, before the processing starts for the first time, and while it continues must:

- review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing;
- except where the processing is based on consent, satisfy 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);
- document decisions as to which lawful basis applies, to help demonstrate compliance with the data protection principles;
- include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
- where sensitive personal information is processed, also identify a lawful special condition for processing that information (see '**Sensitive Personal Information**' section below), and document it; and
- where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

Staff should discuss new processing activity with the Head of Compliance, before embarking on any project or change in system. This will ensure time is built into the process or new system to remain compliant with UK GDPR.

## 6. Sensitive Personal Information

The School may from time to time need to process sensitive personal information. Sensitive personal information will only be processed if:

- there is a lawful basis for doing so as set out above, e.g. it is necessary for the performance of the employment contract, to comply with the School's legal obligations or for the purposes of the School's legitimate interests; and
- one of the special conditions for processing sensitive personal information applies, eg:
  - the data subject has given explicit consent;
  - the processing is necessary for the purposes of exercising the employment law rights or obligations of the School or the data subject;
  - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
  - processing relates to personal data which is manifestly made public by the data subject;
  - the processing is necessary for the establishment, exercise or defence of legal claims; or
  - the processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal information, staff must satisfy themselves that they comply with the criteria noted above and document their decision. Where processing the sensitive data will be for the first time they must notify the Head of Compliance in advance and an assessment must be completed before data is collected or processed.

The School's privacy notices set out the types of sensitive personal information that the School processes, what it is used for and the lawful basis for the processing.

## 7. Processing Safeguarding Information

The School will ensure that staff understand the relevant data protection principles which allow the sharing (and withholding) of personal information including:

- being confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal and should be treated as 'special category personal data'
- understanding that 'safeguarding of children and individuals at risk' is a processing condition that allows the sharing of special category personal data, including without consent where there is good reason to do so. For example, information may be shared without consent where: it is not possible to gain consent; it cannot be reasonably expected to gain consent; and, gaining consent would place a child at risk
- not providing pupils' personal data where the serious harm test is met.

Staff should refer to the [Safeguarding and Child Protection Policy](#) for further information.

## 8. Processing of Financial Information and Credit Card Data

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. Staff who are unsure in this regard must seek further guidance from the Director of Finance. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

## 9. Criminal Records Information

Criminal records information will be processed in accordance with the School's [Safer Recruitment policy](#).

## 10. Data Protection Impact Assessments (DPIA)

Where processing is likely to result in a high risk to an individual's data protection rights (For example, where the School is planning to use a new form of service or system), before commencing the processing, a DPIA to assess must be carried out:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

Before any new form of service or system is purchased, the manager responsible should contact the Head of Compliance in order that a DPIA can be carried out. This process can take some time to complete and therefore engaging with the Head of Compliance early in the decision making or design as possible is important.

Staff are encouraged to also consider the wider safeguarding issues relating to new technology and age appropriate design code, there an assessment must be undertaken to help decide whether to system requires approval from the Head of Compliance or DSL before purchasing. Click here for the [New Software Application/Website/Ed Tec assessment form](#).

The School keeps written records of processing activities and reviews are conducted regularly of the personal information processed and documentation updated accordingly.

## 11. Documentation and Record-Keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to record their own data, and that of others, in a way that is professional and appropriate.

All staff should be aware of the rights of the data subject, whereby any individual about whom information is recorded on School business (notably emails, notes, WHR and CPOMS/ISAMS) may have the right to see that information. This should not discourage staff from recording necessary and sometimes difficult records of incidents or conversation involving colleagues, pupils or parents. Grounds may sometimes exist to withhold these from such requests. The starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.

## 12. Privacy Notices

The School will issue privacy notices from time to time, informing data subjects about the personal information that is collected and held, how they can expect personal information to be used and for what purposes.

We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

It is important that all staff read and comply with the School's privacy notices.

## 13. Individual Rights

All staff have a number of rights in relation to their own personal information which are set out within the Staff Privacy Notice. Any member of staff wishing to exercise any of these rights, should contact the Headmistress.

Individuals are responsible for helping the School keep personal information up to date. Staff should let the HR Department know if the information provided changes, for example a change of address or change details of the bank or building society account. Staff can check and submit personal data through WHR.

## 14. Individual Obligations for online and digital data security

Some staff may have access to the personal information of other members of staff, pupils, parents, suppliers, contractors and Council members of the School in the course of their employment or engagement. If so, the School expects data protection obligations to those individuals are met.

Where staff have access to personal information, they must:

- only access the personal information that they have authority to access, and only for authorised purposes;
- only allow other staff to access personal information if they have appropriate authorisation;
- only allow individuals who are not School staff to access personal information if they have specific authority to do so from their line manager; ;
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions) set out in the School's [Acceptable Use of IT Policy](#);
- not remove personal information, or devices containing personal information (or which can be used to access it), from the School's premises unless appropriate security measures are in place (such as encryption and password protection) to secure the information and the device; and
- not store personal information on local drives or on personal devices.

Staff should contact the Data Breach Team (Bursar, Head of ICT Services and Head of Compliance) – [via this link](#) also available in the staff handbook, if they are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions set out above under the heading '**Sensitive Personal Information**' being met;
- any data breach as set out under the heading '**Data Breaches**' below;
- access to personal information without the proper authorisation;
- personal information not kept or deleted securely;
- removal of personal information, or devices containing personal information (or which can be used to access it), from the School's premises without appropriate security measures being in place; or
- any other breach of this Policy or of any of the data protection principles set out under the heading '**Data Protection Principles**' above.

## 15. Information Security

The School will use appropriate technical and organisational measures in accordance with the School's policies to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

These may include:

- making sure that, where possible, personal information is pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Where the School uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions of the School;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of the School and under a written contract;
- the organisation will assist the School in providing subject access and allowing individuals to exercise their rights under the GDPR;
- the organisation will assist the School in meeting its GDPR obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to the School as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide the School with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the School immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement or process is altered, the relevant line manager must seek guidance of its terms with the Head of Compliance. A Data Privacy Impact Assessment will be required.

In summary the Acceptable Use of IT Policy includes:

- Staff are responsible for the security of the data they have. Measures need to be in place to ensure the security of the data. Acceptable measures include the use of encrypted School devices.
- Use of personal email accounts or unencrypted personal devices by staff for official school business is not permitted.
- The sharing of information should be done using secure systems. See Appendix 1 for further details.

## 16. Storage and Retention of Personal Information

Personal information (and sensitive personal information) will be kept securely in accordance with the School's [Data Retention Policy and Privacy Notices](#).

Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow the School's Data Retention Policy which sets out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult the Head of Compliance.

Limited personal data is retained for archiving purposes where it is necessary to do so in the public interest, for scientific or historical research purposes or statistical purposes subject to appropriate safeguards being put in place to protect the rights and freedoms of the data subject.

## 17. Data Breaches

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure (including power outage);
- human error, such as accidental deletion or alteration of data;
- accidentally sending information to wrong email address;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the person who holds it.

If staff become aware of a data breach or suspect that one has occurred, they must not attempt to investigate themselves. They must immediately report it to the Data Breach Team as soon as possible, within 24 hrs preserving all evidence to the data breach. See Appendix 2 for how a data breach will be handled.

## 18. Subject Access Requests

Any member of staff receiving a request for personal data (either in writing or verbally), must refer it to the Headmistress without any delay and should not acknowledge its receipt until advised to do so by the Data Privacy Lead. Regular reminders for staff on what a subject access can look like are provided.

## 19. International Transfers

The School may transfer personal information outside the UK on the basis that the organisation receiving the information has provided adequate safeguards by way of standard data protection clauses, compliance with this approved code of conduct and the completion of a risk assessment with suitable control measures via a DPIA.



## 20. Training

The School will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or receive subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

## 21. Consequences of failing to comply

The School takes compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal information is being processed;
- carries the risk of significant civil and criminal sanctions for the individual and the School; and
- may, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, an employee's failure to comply with any requirement of it will lead to disciplinary action being considered under School procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If staff have any questions or concerns about anything in this policy, do not hesitate to contact the Head of Compliance.

## 22. Data Governance

The School has an IT Strategy Group (ITSG) which has Data Protection as a standing item on the agenda. Data Breaches which are notified to the ICO are also reported to the Council's Risk Committee.

Member of staff	Bursar / Head of Compliance
Reviewed	August 2023

Version: STDP/v11/23

### Related Policies

Privacy Notices - For Staff, Parents, Pupils, Residents, Seniors and Friends  
Safer Recruitment Policy  
Online Safety Policy  
Social Media Policy  
Acceptable Use of IT Policy (For Staff, Volunteers and Council Members)  
Staff Code of Conduct  
Data Management and Retention Policy  
Biometrics Policy  
CCTV Policy  
Taking, Using and Storing Images of Pupils Policy  
Whistleblowing Policy  
Safeguarding and Child Protection Policy – Sharing of Information

## Data Protection Guidance - Reminders on safely sharing information

### Email:

Sending to “all staff “ put in BCC line (not the To or CC field)

To **avoid** including **personal data** in emails, where possible

To start a **new email** conversation, where possible

To avoid the **Reply All** option

To carefully check that you have the correct recipient. Easy visual checks ... staff have (WA Staff) displayed in their name, in the outlook directory staff names start with first name and include a job title. Pupils emails start with a number and on display you will see their house name.

To **include a link** to either One Drive, SharePoint or Teams areas rather than attachment. (See below) If an attachment is necessary (and includes personal data) password protect the document.

### Email groups:

To be checked by Head of Department at the beginning of each term or when new people start. Contact ICT Helpdesk to correct for you.

### Teams/SharePoint Files and Folders:

The Head of Department / Team Owner to check the Team Members at the beginning of each term and update accordingly. (Teams involving teaching groups is automatically updated via iSAMS)

The default setting for sharing from these areas is set at “**Specific People**”. Sharing with a wider group requires staff to specifically select a different option.

“**People with existing access**” these are for people who will already have access provided as part of the team or teaching group,, or people you have previously shared with.

It is possible to select from the dropdown menu **People in Wycombe Abbey or Anyone in your organisation**. However, please note that by selecting these option gives the recipient the ability to share/distribute to both staff and pupils, including being forwarded on within the organisation. It cannot be shared externally.

### SharePoint Sites:

The default setting will be **Site owners, members and people with edit permission can share files and folders but only site owners can share the entire site**.

*The “Allow access” request **to be switched on for site owners** to allow access when a recipient requests permission.*

**Requesting access for specific people.** This enables you to send to others but you then have to authorise their access, this provides a useful recheck. It also means that the receiving person cannot forward onto anyone else. Only the site owner can do that.

## One Drive:

There are a number of options to share a document.

The default setting is “**Specific People**”. You can change this yourself but you should be aware of the implications:

**People in the Organisation with the link** – Only select when the document does not contain personal or commercial information. This link can be spread amongst Pupils and Staff

**People with exiting access** – this option is for when the document has already been shared with people or groups of people. This link cannot be forwarded to other people.

**Specific People** – This is the safest option but you do need to ensure you select the correct person. Care needs to be taken.

You might also wish to select **block download or restrict editing** .

You can also decide whether recipients can **edit or view**.

**Share and Copy Link** both have the same settings as above. Use **copy link** when you are adding to the content of an email to multiple people.

This option should not be available to select.

**Anyone with the link** – only select when the document does not contain personal or commercial information.

*This link can be spread far and wide, including externally.*

## Handling a Data Breach

The Data Breach Team – Head of Compliance, Bursar and Head of ICT Services will take the following steps:

### Containment and recovery

The Data Breach Team will lead on investigating the breach.

It will be established:

- who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This may include isolating or closing a compromised section of the network, finding a lost piece of equipment and/or changing the access codes;
- whether there is anything that can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back-up hardware to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts;
- which authorities, if relevant, need to be informed.

### Assessment of ongoing risk

The following points will be considered in assessing the ongoing risk of the data breach:

- what type of data is involved?
- how sensitive is it?
- if data has been lost or stolen, are there any protections in place such as encryption?
- what has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relates; if it has been damaged, this poses a different type and level of risk
- regardless of what has happened to the data, what could the data tell a third party about the individual?
- how many individuals' personal data are affected by the breach?
- who are the individuals whose data has been breached?
- what harm can come to those individuals?
- are there wider consequences to consider such as a loss of public confidence in an important service we provide?

### Notification of breach

Notification will take place to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

### Evaluation and response

Once a data breach has been resolved, a full investigation of the incident will take place. This will include:

- reviewing what data is held and where and how it is stored
- identifying where risks and weak points in security measures lie (for example, use of portable storage devices or access to public networks)
- reviewing methods of data sharing and transmission
- increasing staff awareness of data security and filling gaps through training or tailored advice
- reviewing contingency plans

The School will:

- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

This Appendix covers all records - paper, electronic and email. Retention is based on the content of the record, not the format. The Schools Archivist will advise on which documents are to be retained for historical purposes.

### **Destroying records**

Confidential records should always be destroyed securely. Paper records should be shredded. Care should be taken to ensure electronic records are deleted from all areas. Where an external organisation is used to destroy records a certificate of destruction and a summary list of the content should be retained.

## Staff Records (

Information	Retention Period Until	Responsible	Location
Application forms for current staff	Duration of employment plus 7 years	HR	P-File Paper WHR
References received	Duration of employment plus 7 years	HR	P-File Paper WHR
DBS Disclosure Certificate	First Six months of employment	HR	P-File Paper
DBS Disclosure Criminal information	Duration of employment plus 7 years	HR	P-File Paper
Emergency Contact details and Next of Kin	Duration of employment plus 7 years	HR	WHR
Payroll and tax information	Duration of employment plus 7 years	Director of Finance	
Pension related information	Indefinitely where relating to a pension scheme	Director of Finance	
Medical Records/Declarations (except related to accident or injury)	Duration of employment plus 7 years	HR	P-File Paper WHR
Sickness records	Duration of employment plus 7 years	HR	P-File Paper WHR
Annual leave records	Duration of employment plus 7 years	HR	P-File Paper WHR
Unpaid leave / special leave records	Duration of employment plus 7 years	HR	P-File Paper WHR
Appraisal / Assessment / Performance records	Duration of employment plus 7 years	HR	P-File Paper WHR
Records relating to promotion, training etc	Duration of employment plus 7 years	HR	P-File Paper WHR
References given	Duration of employment plus 7 years	HR	P-File Paper WHR
Driver Declarations	Duration of employment	Operations	WHR SharePoint
Car Registration and ANPR	Duration of employment	Custodians	Paxton
Summary of record of service	Indefinitely for archives	HR	WHR

Photographic Image	Duration of employment plus 7 years	HR	WHR
Records relating to accident or injury at work	12 years	Bursar	P-File Paper WHR Accident Log
Disciplinary	Indefinitely or subject to terms of reference	HR	P-File Paper StaffSafe
Safeguarding / Allegations/ Low Level Concerns/Neutral Notifications	Indefinitely	Head	StaffSafe

### Single Central Register

Information	Retention Period until	Responsible	Location
SCR Records	Duration of employment plus 1 complete academic year.	HR	SharePoint

### Unsuccessful Staff Application Records

Information	Retention Period until	Responsible	Location
Application forms and related correspondence	Six months after successful candidate starts	HR	Online Recruitment portal SharePoint
References received	Six months after successful candidate starts	HR	Online Recruitment portal SharePoint

### Staff E-mails (See separate guidance on email protocols and management – Appendix 2, 2.1)

Information	Retention Period until	Responsible	Location
Routine email communications – not stored in other systems, including folders within In Box	Annual data cleanse	Individual Staff	Outlook
Sent Box	Maximum 18 months	IT Auto delete	Outlook
Delete Box	Maximum 90 days	IT Auto delete	Outlook
Email Accounts	Account deleted within 12 months of leaving school	IT	Outlook

*Staff should not rely on email accounts to retain important information, resources, contracts, legal advice, attendance notes, safeguarding concerns or incident reports that ought to be properly held elsewhere (i.e. in the appropriate system – iSAMS, CPOMS, WHR, SharePoint)*

#### Staff video / audio recordings

Information	Retention Period until	Responsible	Location
Lesson recordings	For the duration they are required for teaching, e.g. one term.	Individual Staff	Teams or Zoom
CCTV	Up to 90 days	IT	CCTV Network



**Pupil Records** (\*Where a pupil file is of an historical interest the information may be retained in the School Archives with restricted access.).

Information	Retention period until	Responsible	Location
Application Form, Acceptance Form, Parent Contract and Assessment Results	Until the date of the pupil's 25 <sup>th</sup> birthday	MIS Manager	iSAMS
Academic / educational formal assessments / School Reports eg MIDYiS, ALYS/ performance records	Until the date of the pupil's 25 <sup>th</sup> birthday	MIS Manager Director of Curriculum Management	iSAMS SharePoint
Personal correspondence with pupils or parents - held centrally <i>in Paper or Electronic - SharePoint / CPOMS / iSAMS</i>	Until the date of the pupil's 25 <sup>th</sup> birthday	IT Department	Digital records*
Files held by Housemistresses / HODs /Academic Staff - not required as part of central file	1 year from date of departure	HMs / HODs	SharePoint Paper File
SEND Files - SEN files, reviews & IEPs	Until the date of the pupil's 35 <sup>th</sup> birthday (Keep as separate record files)	Head of Learning Enhancement	CPOMS Digital Records*
Internal examination papers (Policy from 2017 is to return papers to pupils)	2 years from date of examination	HODs	Paper Files/SharePoint
Internal examination results	Until the date of the pupil's 25 <sup>th</sup> birthday	MIS Manager	iSAMS SharePoint
Public Examination results and school achievements registers – held separate to pupil file	Held for 7 years	Examinations Office	SharePoint iSAMS
UCAS forms – add to central file	Until the date of the pupil's 25 <sup>th</sup> birthday	Director of Sixth Form	Digital Record*
Other references given – add to central file	Until the date of the pupil's 25 <sup>th</sup> birthday	Heads Office	Digital Record*
Records relating to accident or injury at School	Until the date of the pupil's 25 <sup>th</sup> birthday	Bursar	Accident Log CPOMS
Work Experience agreement – add to central file	Until the date of the pupil's 25 <sup>th</sup> birthday	Work Experience Coordinator	Digital Record*
Health Records (Electronic)	Until the date of the pupil's 25 <sup>th</sup> birthday	Health Centre Manager	iSAMS

Medical card – returned to pupils on leaving			
Safeguarding / Child Abuse	Indefinitely	DSL	CPOMS Digital Vault
Bullying	In line with policy/agreement note on pupil file as required.  LOGS – Incident + 10 years	Deputy Head (Pupils)	SharePoint (LOG)  CPOMS
Sanctions incl Exclusion	In line with policy/agreement note on pupil file as required.  LOGS – Incident + 10 years	Head	SharePoint (LOG)  CPOMS
Letters Authorising Absence	Date of Absence + 2 years	Head	SharePoint
UKVI Child Student	Until 1 year after pupil has left or end of Visa.	DH (Pupils)	iSAMS
Passport	Until 1 year after pupil has left	DH(Pupils)	iSAMS
Physical Restraint LOG		DH (Pupils)	SharePoint

#### Minutes of meetings & associated reports

Information	Retention period until	Responsible to retain the single central version	Location
ELT	Date of Meeting + 6 years  (A selection will be retained by the School Archivist)	Head	SharePoint
HODs		DH (Academic)	
SoT		DH	
Staff Briefings		Head	
Academic Staff Meetings		DH (Academic)	
Reports by ELT, HoYs, HoDs or other		Head	
Safeguarding Team Meeting Minutes	Indefinite	Director of Safeguarding	SharePoint
Governing Council Committees	Permanent	Bursar	SharePoint

#### School specific records

Information	Retention period until	Responsible to retain the single central version	Location
School development plan	Date of completion of Plan + 6 years  (A selection will be retained by the School Archivist)	Bursar	SharePoint/Hard Copy
Curriculum plan		DH (Academic)	
Pastoral plan		DH (Pupils)	
Department development plans		DH (Academic)	

#### ISSRS related documents

Information	Retention period until	Responsible	Location
Policy Documents	Permanent Record	Head of Compliance	SharePoint
ISI Reports and Notices	Permanent Record	Head	SharePoint
Annual Census – DFE, ISI	Date of report plus 10 years	DH (Pupils)	SharePoint
Complaints Log/Files	Date of Complaint resolution + 6 years (or longer if deemed appropriate by Bursar)	Head	SharePoint
Search Logs	In line with policy/agreement - note on pupil file as required.  LOGS – Incident + 10 years	DH (Pupils)	SharePoint
Physical Restraint Logs	Incident + 10 years	DH (Pupils)	SharePoint
Bullying Log/Files	In line with policy/agreement - note on pupil file as required.  LOGS – Incident + 10 years	DH (pupils)	SharePoint CPOMS
Sanctions incl Exclusion	In line with policy/agreement note on pupil file as required.  LOGS – Incident + 10 years	Head	SharePoint (LOG) CPOMS
Admissions Register	Permanent Record  (Reduced after 6 years for pupils on roll)	MIS Manager	iSAMS

Attendance Registers	Date of register plus 3 years	MIS Manager	iSAMS
Attendance Returns	Academic year plus 1	DH Pupils	SharePoint
LA submission Leavers Information	Until the date of the pupil's 25 <sup>th</sup> birthday	DH Pupils	CPOMS
Accident Logs	Pupils – 25 years from birth Staff – min 4 years	Head of Compliance	CPOMS SharePoint
Visiting Speaker Logs	Academic Year plus 2	Director of Safeguarding	SharePoint
Visitors Log	Academic Year plus 1	Bursar	Sign In App/Visitors Book

#### Communications (not mentioned elsewhere)

Information	Retention period until	Responsible	Location
Mailing - including circulars such as newsletter	Permanent Record	Head of Communications	School Post/My School Portal
Correspondence (Heads Office)	Until the date of the pupil's 25 <sup>th</sup> birthday	Head	CPOMS
Operational Correspondence – Houses /Departments	Until no longer relevant	HMs, HODs, LMs	Operational Files in SharePoint
School Events (including eg those with external visitors, pupils from other schools, prospective pupils)	Programme and attendee list – Date of event plus 7 years or Archives	Events Manager	SharePoint Archives
Pupil/Staff Images of activities and events	Part of school archives of events and activities	Head of Communications	SharePoint Archives Planet E-Stream

#### Trip Information (not mentioned elsewhere)

Information	Retention period until	Responsible	Location
Parental Permission Slips for trips	Until conclusion of trip	EVC	Evolve/SharePoint
If major incident on trip	DoB of pupil involved + 25 yrs	Bursar	SharePoint
Record created by school to obtain approval to run an Educational Visit outside the classroom with participants list	Date of Visit plus 10 years	EVC	SharePoint

### Admissions (not mentioned elsewhere)

Information	Retention period until	Responsible	Location
Successful applicants	As part of pupils file: Until the date of the pupil's 25 <sup>th</sup> birthday	EVC	iSAMS
Unsuccessful applicants	Resolution plus 1 year	Director of Admissions	iSAMS
Entry Assessments	Resolution plus 1 year with names; Anonymise after	Director of Admissions	SharePoint

### Academic Work / Teachers Records

Information	Retention period until	Responsible	Location
Department Syllabus	Current Year +1 yr	HOD	SharePoint
SoW	Current Year + 1yr	HOD	SharePoint
Timetable	Current Year +1 yr	MIS Manager	iSAMS
Mark Books	Current year +2 yr	Ind Teachers	SharePoint
Record of prep set	Current Year + 1 yr	Ind Teachers	SharePoint
Pupils' Work – Return where possible	Current Year	Ind Teachers	SharePoint

### Corporate Records

Information	Retention period until	Responsible	Location
Certificate of incorporation	Permanent	Bursar	SharePoint
Register of Members/Council	Permanent	Bursar	SharePoint
Annual Report	Permanent	Bursar	SharePoint
Deeds	Permanent	Bursar	SharePoint
Contracts	Permanent	Bursar	Share Point

### Financial Records

Information	Retention period until	Responsible	Location
Accounting Records	6 years	Director of Finance	Sage/iFinance

Tax Returns	6 years	Director of Finance	SharePoint
VAT Returns	6 years	Director of Finance	SharePoint
Payroll. Salary, maternity pay records	6 years	Director of Finance	Iris and SharePoint
Pension	Permanent	Director of Finance	Iris and SharePoint
Internal Financial Reports	3 or 6 years	Director of Finance	SharePoint
Gift Register	6 years	Bursar	SharePoint
Parent Invoices	7 years	Director of Finance	Sage/iFinance/SharePoint

#### Estates Records

Information	Retention period until	Responsible	Location
Maintenance / Inspections Logs	10 yrs	Estates Manager	SharePoint or Parago
Building Manuals/Drawings/Plans	Permanent	Estates Manager	SharePoint
Fire Actions, FRAs and Drill records	Life of building/Permanent	Estates Manager	SharePoint
H&S Committee Minutes	Permanent	Bursar	SharePoint
Documentation – Hazardous substances/Health Surveillance records	40 years	Estates Manager	SharePoint and Estates Archives

#### Development Records

Information	Retention period until	Responsible	Location
Seniors Records	Permanent	Director of Development	Raisers Edge
Friends of WA Records	Permanent (Opt In)	Director of Development	Raisers Edge
Current Parents	Permanent	Director of Development	Raisers Edge
Correspondence/Letters/Emails	Permanent	Director of Development	Raisers Edge

Donations/Financial Information	Permanent	Director of Development	Raisers Edge
---------------------------------	-----------	-------------------------	--------------

#### ICT Records

Information	Retention period until	Responsible	Location
IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement	Head of ICT Services	9nine or SharePoint

#### Business Records

Information	Retention period until	Responsible	Location
Data Protection Logs/Audits/Record of Processing	Permanent	Head of Compliance	SharePoint
Service Level Agreements	Until superseded	Bursar	SharePoint
Contracts	Until superseded	Bursar	SharePoint
Insurance Policies and Correspondence	Permanent	Bursar	SharePoint
Risk Assessments	7 years from completion		SharePoint
Consultation Records	6 years from consultation end	Bursar	SharePoint

#### School Shop Records

Information	Retention period until	Responsible	Location
New Pupil Uniform Ordering information including parent addresses	Start date plus 1 year	Shop Manager	SharePoint

Additional Guidance Available:

[Boarding House Data Retention Guidance](#)

Member of staff	Bursar
Reviewed	August 2023



## Appendix 2

### Data Management – Guidance for staff

---



The Schools follows a protocol of regularly reviewing the data that is held across all areas of the business to ensure only necessary and accurate data is retained, aiming to hold one single version of the data in a central location. The storage and retention schedule (Appendix 1) is a list of the minimum records the School must keep.

#### 1. Retaining Data for the right reason

There are four main reasons for keeping data. The watchwords of record-keeping are accuracy, clarity, professionalism and objectivity.

##### 1.1 The Law

In some instances there is a law which specifies how long something should be kept for. This is particularly true where matters of health and safety are concerned, but can also apply to contracts, expenditure and immigration. Where there is not a specific law we often look to the Limitation Act 1980. This is the Act that allows people 6 years after a contract has been broken to take their case to court.

##### 1.2 Business Continuity

The School needs to have evidence we know about our pupils, our academic and support departments and our facilities. There is also business continuity on an individual level and if a staff member left tomorrow the School will require records that would allow someone else to step into your role – written procedures, lists of contacts, and so on. In a specific job role there will be things that you are not done very often and older documents need be kept as a reminder of how things were done as a template.

##### 1.3 Work in progress

There will also be materials that need to be kept because they are in progress or part of an ongoing conversation. These will probably need to be kept while the work is in progress. At the end, staff should keep a note of the final outcome of the investigation, the final report, policy or approved set of minutes. The final version should be held in a central official School location.

##### 1.4 Historical interest

The School is a live working business, not a museum, and has to strike a balance between respecting its history and being swamped by it. The Library and archivist keeps files on the main events in the history of the School.

#### 2. Data Cleansing and good housekeeping

You are asked to annually review and cleanse their specific individual work spaces including emails, OneDrive, SharePoint and files. The School utilises MSOffice Compliance to perform automatic deleting and cleansing.

##### 2.1 Email Protocols and Management

You are encouraged to consider the following principles when managing your emails.

- Read, note/action and **delete**.

- **Permanently Keep** - File in an appropriate School system – CPOMS, iSAMS, WHR, SharePoint etc.
- **Ongoing conversations** – hold within outlook until conversation is completed. Up to one year.

The following settings are in place:

- automatic deleting of the **delete box** for information dated over 90 days.
- automatic deleting of the **sent box** after 18 months.
- there is a limited **cap on data storage**. IT to set and review on an individual basis.
- subfolders within **IN Box should not be created** beyond ongoing conversations
- **monitoring of email** traffic containing personal or sensitive data will continue

Any **additional Email boxes** to be reviewed by IT and Data Lead on an annual basis.

Staff should not rely on email accounts to retain important information, resources, contracts, legal advice, attendance notes, safeguarding concerns or incident reports that ought to be properly held elsewhere (i.e. in the appropriate system – iSAMS, CPOMS, WHR, SharePoint)

## 2.2 Space saving

The School needs space for teaching facilities, for offices and meetings. Work space is more comfortable when there are not piles of paper sliding over the desk, a filing cabinet wedged in and boxes of files under the desk. Electronic documents might feel as though they take up no space, but they take up electronic space on cloud servers that have to be bought, maintained, backed up and upgraded, and which use electricity. Electronic files can be a matter of “out of sight, out of mind” and staff are encouraged to try to remember that they needed to be weeded out on a regular basis.

## 2.3 Time

All of us have spent time hunting for things that we know we’ve put somewhere, but just cannot find. And of course if something is badly misfiled (or unfiled, in a pile) it is for all intents and purposes, lost.

## 2.4 Version control

All staff are asked to consider the importance of a single version of a document. The final version should be the one filed in the Schools central system. Staff are asked to throw out old versions (including drafts) and label new documents with a date.

## 2.5 Subject Access Request

A subject access request is where a pupil, staff member or parent, whether current or past, can ask to see all the information we hold that relates to them. We have just 1 month to respond to the request. That includes finding all the information, copying it and redacting other people’s data. A subject access request can be limited by our retention policy so make sure that you are not keeping information for longer than necessary, and to help save time looking keep the information in the correct central School location.

## 2.6 Freedom of Information

The Freedom of Information Act does not apply to us as an Independent School.

## 2.7 Data Protection

than is necessary. Please refer to the Storage and retention of data guidance for detailed listing of records – Appendix 1.

## 3. Further Guidance

Further guidance on retention and disposal of records should be referred to the Head of Compliance.

Member of staff	Bursar
Reviewed	August 2023

