Data Protection Policy for Staff

Data protection is an important compliance issue for the School. During the course of the School's activities personal data 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 General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA2018). The Information Commissioner's Office (ICO) is responsible for enforcing data protection law.

1. APPLICATION OF THIS POLICY

This policy applies to current staff, including employees, workers, volunteers, apprentices, Council members and contractors (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.

This policy will be reviewed and updated in accordance with data protection obligations. It does not form part of any contract of employment and may be amended, updated or supplemented from time to time.

All staff 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.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be 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 third party data controllers – which may range from other schools, universities, parents, to appropriate authorities - 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 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 Abbe 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 may result in disciplinary action. 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.

4. 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 information" 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.

5. 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

- proceed 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 our 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.

6. BASIS 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.

In relation to any processing activity will, before the processing starts for the first time, and while it continues:

- review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:
    - that the data subject has consented to the processing;
    - that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    - that the processing is necessary for compliance with a legal obligation to which the School is subject;
    - that the processing is necessary for the protection of the vital interests of the data subject or another natural person;
    - that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority;
    - that the processing is necessary for the engagement of contractors or the engagement of services; or
    - that the processing is necessary for the purposes of legitimate interests of the School or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
- 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.

7. 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, e.g.:
    - 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 for the first time they must notify the Head of Compliance and an assessment must be completed.

Sensitive personal information will not be processed until:

- the assessment referred to above has taken place; and
- the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

When determining whether the School's legitimate interests are the most appropriate basis for lawful processing, will:

- conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure justification of the decision;
- if the LIA identifies a significant privacy impact, conduct a data protection impact assessment (DPIA);
- keep the LIA under review, and repeat it if circumstances change; and
- include information about our legitimate interests in our relevant privacy notice(s).

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.

8. Processing of 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.

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), we will, before commencing the processing, carry out a DPIA to assess:

- 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 must complete an assessment form to help decide whether to system requires approval from the Head of Compliance or DSL before purchasing. Click here for the New Software Application assessment form.

The School keeps written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:

- the purposes of the processing;
- a description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;
- where possible, retention schedules; and
- where possible, a description of technical and organisational security measures.

Where sensitive personal information or criminal records information is prcessed, written records are kept of:

- the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
- the lawful basis for our processing; and
- whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

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.

14. Individual Obligations

Individuals are responsible for helping the School keep their 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 will have the option to check and submit personal data through WHR.

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. For example, staff should be aware that they also enjoy the rights set out above.

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 Compliance Manager) – 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.

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.

The Data Breach Team 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.

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. The Head of Compliance provides regular training for staff on what a subject access can look like.

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 and of compliance with an approved code of conduct.

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 responding to 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 may lead to disciplinary action 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. The Head of Compliance organises a twice–yearly "User Group" meeting of data champions from various departments who handle large volumes of personal data. The purpose of the group is to review anonymised data breach reports to understand issues, consider best practice, suggest further developments to improve data systems and receive training. Notes from the user group meetings are fed into the ITSG.

Data Breaches which are notified to the ICO are also reported to the Risk Committee.

Member of staff	Bursar / Head of Compliance
Reviewed	August 2021

VERSION: STDP/v8/21

Related Documents:

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