Data Protection Policy

Contents

1. Introduction 2
2. Definitions 3
3. Responsibility for Data Protection 4
4. Data Protection Principles 4
5. Lawfulness, Fairness and Transparency 5
6. Limitation, Minimisation and Accuracy 6
7. Special Category and Criminal Offence Data 6
8. Sharing Personal Data 8
9. Subject Access Requests 9
10. Other Rights of Individuals 11
11. Biometric Recognition Systems 12
12. CCTV 12
13. Photographic and video images 12
14. Data Protection by Design and Default 13
15. Data Security and Storage of Records 14
16. Disposal of Records 15
17. Personal Data Breaches 15
18. Training 15
19. Processing of Credit Card Data 16
20. Complaints 16
21. Related Policies 16
22. Review 17

1. Introduction

Data protection is an important legal compliance issue for the King's School, Worcester Foundation (the Foundation). During the course of the Foundation's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, parents/guardians, contractors and other third parties (in a manner more fully detailed in the Foundation's Privacy Notice).

The Foundation is registered as a Data Controller, ICO registration number Z7022029. The registration is renewed annually. The Foundation, as a 'Data Controller', is liable for the actions of its staff, volunteers and Governors in how they handle data. It is therefore an area where all staff, volunteers and Governors have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and

regarding the right of access to personal data.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law. These can include a significant fine for a serious breach.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Definitions

Data Controller
An organisation that determines the purpose and means of the processing of personal data. For example, the Foundation is the controller of pupils' personal information. As a Data Controller, the Foundation is responsible for safeguarding the use of personal data.

Data processor
An organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

Data subject
The identified or identifiable individual whose personal data is held or processed.

Personal data breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Personal information (or personal data)
Any information relating to a living individual (a data subject) by which (on its own, or when added to other information) that individual may be identified. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles, usernames or nicknames. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the Foundation's, or any person's, intentions towards that individual.

Processing
Anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it. Processing can be automated or manual.

Special categories of personal data (sensitive data)
Personal data which is more sensitive and so needs more protection, including data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetics, or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences. More information is given in section 7 of this policy.

3. Responsibility for Data Protection

This policy applies to **all staff** employed by the Foundation, and to external organisations or individuals working or volunteering on behalf of the Foundation. Staff who do not comply with this policy may face disciplinary action.

The Governing Body has overall responsibility for ensuring that the Foundation complies with all relevant data protection obligations.

The Foundation has appointed an external Data Protection Officer (DPO) – SchoolPro TLC Limited (SchoolPro). SchoolPro is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. Full details of the DPO's responsibilities are set out in their SLA. SchoolPro can be contacted via DPO@SchoolPro.uk

The Foundation has appointed a Compliance Manager as the Data Protection Lead who will deal with requests and enquiries and consult with our external Data Protection Officer as required. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Compliance Manager via compliance@ksw.org.uk.

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Foundation of any changes to their personal data, such as a change of address
- Contacting the Compliance Manager in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

4. Data Protection Principles

The UK 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:

1. Processed **lawfully**, **fairly** and in a **transparent** manner
2. Collected for **specific, explicit and legitimate purposes** and processed only for the purposes it was collected for
3. **Adequate, relevant** and **limited** to what is necessary to fulfil the purposes for which it is processed
4. Accurate and kept up to date

5. **Kept for no longer than is necessary** for the purposes for which it is processed
6. Processed in a manner that ensures **appropriate security** of the personal data.

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

- keeping records of our data processing activities, including by way of logs and policies
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments)
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our 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. Lawfulness, Fairness and Transparency

Under the UK GDPR there are several different lawful grounds for processing personal data:

- The data needs to be processed so that the Foundation can **fulfil a contract** with the individual, or the individual has asked the Foundation to take specific steps before entering into a contract
- The data needs to be processed so that the Foundation can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the Foundation can perform a task in the **public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Foundation or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/guardian when appropriate in the case of a pupil) has freely given clear **consent**

For further detail on which lawful basis is used for each category of data, see the relevant privacy notice.

For special categories of personal data, the Foundation will also meet one of the special category conditions for processing, which are set out in the UK GDPR and Data Protection Act 2018. More information is given in section 7 of this policy.

If online services, such as classroom apps, are offered to pupils, the Foundation will rely on Legitimate Interest as the basis for processing. Where this is not appropriate, consent will be obtained for processing (except for online counselling and preventative services).

Whenever personal data is first collected directly from individuals, the Foundation will provide them with the relevant information required by data protection law.

The Foundation will only collect personal data for specified, explicit and legitimate reasons and will always endeavour to ensure that there are lawful grounds for processing personal information. If personal data is to be used for reasons other than those given when it was first obtained, the

Foundation will inform the individuals concerned before this is done and seek consent where necessary.

6. Limitation, Minimisation and Accuracy

The Foundation endeavours to ensure that data is not kept for longer than necessary. Data is destroyed securely as soon as reasonably practicable and in accordance with the Foundation's Data Retention Policy. The Foundation may retain personal data indefinitely to comply with regulatory or legal obligations and for legitimate organisational reasons.

It is important that personal data held by the Foundation is accurate, fair and adequate. Individuals must inform the Foundation if they believe that any personal data is inaccurate or untrue or if they are dissatisfied with the information in any way. A person may have the right to request that inaccurate information about them is erased or corrected, depending on the nature of the information and the basis on which that data is processed.

7. Special Category and Criminal Offence Data

As part of our statutory functions, we process special category data and criminal offence data in accordance with the requirements of Articles 9 and 10 of the UK GDPR and Schedule 1 of the DPA 2018.

Special Category Data

Special category data is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

Criminal Conviction Data

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Appropriate Policy Document

Some of the Schedule 1 conditions for processing special category and criminal offence data require the Foundation to have an Appropriate Policy Document (APD) in place, setting out and explaining the procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This section of the Data Protection Policy explains this processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about the processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements the Foundation's privacy notices.

Conditions for processing special category and criminal offence data

We process special categories of personal data under the following UK GDPR Articles:

- Article 9(2)(a) – explicit consent

  In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

  Examples of our processing include staff and pupil dietary requirements and health information we receive from our staff and pupils who require a reasonable adjustment to access our services.

- Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Foundation or the data subject in connection with employment, social security or social protection.

  Examples of our processing include staff sickness absences, tax and National Insurance data.

- Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.

  An example of our processing would be using health information about a pupil or member of staff in a medical emergency.

- Article 9(2)(f) – for the establishment, exercise or defence of legal claims.

  Examples of our processing include processing relating to any employment tribunal or other litigation.

- Article 9(2)(g) - reasons of substantial public interest.

  The Foundation provides a safeguarding role to young and vulnerable people. The processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role.

  Examples of our processing include the information sought, provided or received (e.g. from the local authority) as part of investigating an allegation.

- Article 9(2)(j) – for archiving purposes in the public interest.

  The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – archiving.

  An example of our processing is the transfers we may make to the County Archives as set out in our Data Retention Policy.

Criminal offence data is processed under Article 10 of the UK GDPR.

Examples of the processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations, and sharing information as required, for example with a local authority or the Department for Education re 'the Barred List' .

Processing which requires an Appropriate Policy Document

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the APD for the Foundation. It demonstrates that the processing of special category (SC) and criminal offence (CO) data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. Data retention with respect to this data is documented in the Data Retention Policy.

Description of data processed

Special category data about our employees that is necessary to fulfil our obligations as an employer is processed. This includes information about their health and well-being, ethnicity, photographs and their membership of any union. Further information about this processing can be found in the Privacy Notice.

Special category data about the children in our care and other members of our community that is necessary to fulfil our obligations as a Foundation, and for safeguarding and care, is processed. This includes information about their health and well-being, ethnicity, photographs and other categories of data relevant to the provision of care. Further information about this processing can be found in the Privacy Notice.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Schedule 1 conditions for processing

Special category data

Special Category data is processed for the following purposes in Part 1 of Schedule 1:

- Paragraph 1(1) employment, social security and social protection.

Special Category data is processed for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- Paragraph 6(1) and (2)(a) statutory, etc. purposes
- Paragraph 18(1) – safeguarding of children and of individuals at risk.

Criminal offence data

Criminal offence data is processed for the following purposes in parts 1, 2 and 3 of Schedule 1:

- Paragraph 1 – employment, social security and social protection
- Paragraph 6(2)(a) – statutory, etc. purposes
- Paragraph 12(1) – regulatory requirements relating to unlawful acts and dishonesty etc.
- Paragraph 18(1) – safeguarding of children and of individuals at risk
- Paragraph 36 – Extension of conditions in part 2 of this Schedule referring to substantial public interest.

8. Sharing Personal Data

The Foundation will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/guardian that puts the safety of Foundation staff or other pupils/children at risk
- There is a need to liaise with other agencies – consent may be sought if necessary or appropriate before doing this. Consent may not be obtained if to do so would put at risk the safety of another individual.

- The Foundation's suppliers or contractors need data to enable the Foundation to provide services to staff, volunteers and pupils – for example, IT and communication companies, education support companies, and those that provide tools for learning. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

Personal data may also be shared with emergency services and local authorities to help them to respond to an emergency situation that affects any of the Foundation's pupils, volunteers or staff.

Where personal data is transferred to a country or territory outside the European Economic Area, it will be done in accordance with data protection law.

9. Subject Access Requests

Individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that the Foundation holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested.

If staff receive a subject access request, they must immediately forward it to the Compliance Manager.

Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or guardians. For a parent or guardian to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or guardians of pupils at the Prep Schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Where a pupil raises a concern confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents/guardian the Foundation will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the Foundation believes disclosure will be in the best interests of the pupil or other pupils.

Responding to Subject Access Requests

When responding to requests, the Foundation:

- may ask the individual to provide 2 forms of identification
- may contact the individual via phone to confirm the request was made
- will respond without delay and within 1 month of receipt of the request
- will provide the information free of charge
- may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

The Foundation will not disclose information if it:

- might cause serious harm to the physical or mental health of the pupil or another individual
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- is contained in adoption or parental order records
- is given to a court in proceedings concerning the child.

The Foundation will not provide copies of examination scripts, or provide examination marks before they are officially announced. The Foundation will generally not be required to provide access to information held mutually and in an unstructured way.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When a request is refused, the individual will be told why, and will be told that they have the right to complain to the ICO.

The UK GDPR does not prevent a data subject making a subject access request via a third party. Requests from third parties are dealt with as follows:

- In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the data subject.
- 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.
- If there is no evidence that the third party is authorised to act on behalf of the data subject, we are not required to respond to the SAR.
- However, if it is possible to contact the data subject directly, we will do so to confirm whether they wish to make a SAR.

10. Other Rights of Individuals

In addition to the right to make a subject access request, individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate
- request that we erase their personal data (in certain circumstances)
- request that we restrict our data processing activities (in certain circumstances)
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used, machine-readable format to another data controller (in certain circumstances)
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.
- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention)
- object to the use of their personal data for direct marketing
- request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- be notified of a data breach (in certain circumstances)
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent)
- make a complaint to the ICO.

Individuals should submit any request to exercise these rights to the Compliance Manager. If staff receive such a request, they must immediately forward it to the Compliance Manager.

It is important to note that the Foundation could be reported to the Information Commissioner's Office for failure to comply with their statutory responsibilities regarding SARs and other data protection rights of the individual, and penalties (including financial) may apply.

11. Biometric Recognition Systems

The Foundation does not collect or otherwise process biometric data.

12. CCTV

The Foundation uses CCTV in various locations around the school sites to ensure they remain safe. We adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Further information is given in the Foundation's CCTV Policy.

13. Photographic and video images

The Foundation may use photographs or video of pupils in the following ways:

- For the purpose of holding a digital formal identity photograph of each pupil for pastoral and administrative purposes which do not include publicity.
- Unless the relevant individual objects in writing and subject to the exception in italics, the Foundation may also
    - Publish photographs or video in
        - Foundation publications. (For example, e- bulletins, newsletters, social networking services and the Foundation's website) to support teaching and learning, to celebrate pupil achievement and for Foundation publicity, and
        - Foundation promotional material (For example, the prospectus). *However, named captioned individual portraits of pupils or pupil addresses will not be published by the Foundation without the appropriate person's express written consent.*
    - Publish photographs of Foundation events, which may include images of groups of parents/guardians, alumni or other visitors to show an activity to better effect. *However, the Foundation will not publish a name captioned individual portrait photograph without the express written consent of the relevant individual.*
    - Allow third party media (for example, visiting journalists) to use photographs or video for their own journalistic purposes. *However, individual pupil portraits (whether or not they include a caption with the pupil's name) will not be published by third party journalists without the express written consent of the relevant individual.*

On joining the Foundation, parents/guardians are invited to indicate whether they consent or object to the use of images and video for various further purposes via the Acceptance Form. After this, the relevant person can choose to amend their preferences by writing to the Compliance Manager using the contact details below. Any changes made to your preferences will take effect from the date we issue our written acknowledgement.

Where consent is withdrawn, the Foundation will make reasonable efforts to ensure that the image is not used in future. However, it may not always be possible to remove images/video that have already been published or circulated.

Where parents/guardians and others attend Foundation performances and sporting events etc the Foundation will generally (but not always) permit reasonable photography or video recording for personal domestic purposes only. However, the Foundation does not permit the publishing or any photograph or video recording of children other than your own. This includes publishing on social networking sites such as Facebook and YouTube. The Foundation's policy reflects our legal obligation to protect the privacy and in some cases personal safety of all of our pupils and recognises that not all pupils and parents/guardians wish or consent to their images and other personal data being published.

14. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 4)
- Completing Data Protection Impact Assessments (DPIAs) where the Foundation's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the Foundation and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

Data Protection Impact Assessments (DPIAs)
A Data Protection Impact Assessment is a process to help us identify and minimise the data protection risks of a project.

We will complete a DPIA for processing that is likely to result in a high risk to individuals as well as any other major project which requires the processing of personal data.

It is vital that the DPIA is completed before processing is commenced to ensure that all risks are identified and mitigated as much as possible.

Our DPIA will:

- describe the nature, scope, context, and purposes of the processing
- assess necessity, proportionality, and compliance measures
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

To assess the level of risk, we will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

We will consult our data protection officer (SchoolPro TLC Ltd) and, where appropriate, individuals and relevant experts. We may also need to consult with relevant processors.

If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing.

We will implement the measures we identified from the DPIA, and integrate them into our policies, procedures, and practice.

15. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must follow the relevant procedures and ensure all records and copies are returned to a school site.
- Passwords that are at least 12 characters long containing letters, numbers and special characters are used to access Foundation computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

- Staff, pupils or Governors who store personal information on their personal devices are expected to follow the same security procedures as for Foundation-owned equipment (see the Foundation's Acceptable Use Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

The King's School Worcester archive is maintained as a resource to help inspire and equip current staff and pupils to understand and appreciate issues of identity, belonging and shared heritage; to prompt memories of school-life among many generations of Old Vigornians; and to serve as a research resource for all interested in the history of The King's School and the community it serves.

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. This is with the exception of data that is retained in our Foundation archive as described in section 15.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Foundation's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Further information is given in the Foundation's Data Retention Policy.

17. Personal Data Breaches

The Foundation will make reasonable endeavours to ensure that there are no personal data breaches.

In the event of a suspected data breach, we will follow the procedure set out in the Foundation's Data Breach Procedure.

When appropriate, we will report the data breach to the ICO within 72 hours. Examples of possible breaches in a school context might include, but are not limited, to:

- A non-anonymised dataset being published on the Foundation website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a Foundation-owned laptop containing non-encrypted personal data about pupils

It is important to note that the Foundation could be reported to the ICO for high risk data breaches and penalties (including financial) may apply.

18. Training

All staff and Governors are provided with data protection training as part of their induction process.

Data Protection will also form part of continuing professional development, where changes to legislation, guidance or the Foundation's processes make it necessary.

19. Processing of Credit Card Data

The Foundation 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. 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.

20. Complaints

If you have any queries or complaints concerning your personal data or any question about this policy, please contact the Foundation's Compliance Manager:

Email: compliance@ksw.org.uk

Telephone: 01905 721700

Post: The King's School, 5 College Green, Worcester, WR1 2LL

You may also contact the Foundation's external DPO, SchoolPro TLC,

Email: contact@schoolpro.uk

Telephone: 0203 2909093

Post: SchoolPro TLC, Midway House, Staverton Technology Park, Cheltenham, GL51 6TQ

21. Related Policies

- Privacy Notice
- Acceptable Use Policies
- Safeguarding Policy
- Behaviour Management Policy
- Staff Code of Conduct
- CCTV Policy
- Data Breach Procedure
- Data Retention Policy

22. Review

This policy will be reviewed annually with key stakeholders.

Authorised by	Resolution of the Governors
Signature	
Date Adopted	22 March 2024
Revised on	07 February 2024
Review due	01 February 2025
Circulation	Members of Governors/ all staff / parents / pupils [on request]