Data Protection Policy

Contents

1. Introduction 3
2. Accessibility Statement 4
3. Definitions 4
4. Scope and Responsibilities 5
5. Responsibility for Data Protection 6
6. Data Protection Principles 7
7. Lawfulness, Fairness and Transparency 7
8. Limitation, Minimisation and Accuracy 8
9. Processing of Special Category and Criminal Offence Data 8
10. Sharing Personal Data 9
11. Subject Access Requests 12
12. Other Rights of Individuals 14
13. Biometric Recognition Systems 15
14. CCTV 15
15. Photographic and Video Images 16
16. Artificial Intelligence (AI) 17
17. Data Protection by Design and Default 18
18. Data Security and Storage of Records 19
19. Disposal of Records 19
20. Personal Data Breaches 20
21. Training 20
22. Processing of Credit Card Data 20
23. Complaints 21
24. Related Policies 21
25. Version Control 22
26. Approval 22

1. Introduction

Data Protection is an important legal compliance responsibility for the King's School, Worcester Foundation ("the Foundation"). The Foundation collects, stores and processes personal data - including sensitive information - about staff, pupils, parents/guardians, Governors, alumni, donors, visitors, job applicants, hirers of our facilities, contractors and others. Full details of how personal data is used are provided in the Foundation's Privacy Notices.

The Foundation is registered with the Information Commissioner's Office (ICO) as a Data Controller, (registration number: Z7022029). As a Data Controller, the Foundation is legally responsible for the actions of its staff, volunteers and Governors in how they handle personal data. All individuals involved in the Foundation's operations have a duty to ensure that data is processed lawfully, securely, and with respect for individuals' rights.

The Foundation complies with the following legislation in respect of data protection:

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- **Data (Use and Access) Act 2025**

These laws strengthen the rights of individuals and impose strict obligations on organisations that process personal data, including schools. The Information Commissioner's Office (ICO) enforces these laws and investigates complaints free of charge. It has powers to take action against breaches, including issuing significant fines.

This policy is intended for staff, Governors, parents, pupils, members of the public and others who wish to understand how the Foundation handles personal data. It applies to all personal data, whether in paper or electronic format.

Disclaimer

This policy has been prepared for internal use by The King's School, Worcester Foundation and reflects current data protection legislation and best practice guidance as of October 2025. It is not intended to constitute legal advice and should not be relied upon as such. The Foundation recommends seeking independent legal advice where specific data protection concerns or contractual arrangements arise.

The examples of data processing activities described in this policy are illustrative and not exhaustive. The Foundation may carry out other forms of processing where lawful and appropriate, in line with this policy and applicable data protection legislation.

This document may be updated periodically to reflect changes in law or regulatory guidance.

2. Accessibility Statement

The King's School, Worcester is committed to making our privacy notices accessible to everyone. If you require this document in an alternative format - such as large print, Braille, audio, or another language - please contact the Compliance Manager at compliance@ksw.org.uk or by telephone. We will do our best to provide the information you need in a way that works for you.

3. Definitions

Data Controller

An organisation that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the Foundation is the Data Controller of pupils' personal information. As a Data Controller, the Foundation is responsible for safeguarding the use of personal data. An independent contractor, such as a peripatetic music teacher, who makes their own decisions is also, separately, likely to be a Data Controller.

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. They must act only on documented instructions from the Data Controller and are subject to contractual obligations under Article 28 of UK GDPR.

Data Subject

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

Criminal Offence Data

Personal data relating to criminal convictions, offences, or related security measures. This is subject to additional safeguards under Article 10 of UK GDPR and Schedule 1 of the Data Protection Act 2018.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include sending personal data to the wrong recipient, loss of a device containing personal data, or unauthorised access by a third party.

Personal Data

Any data 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

Virtually 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 separate rules for the processing of personal data relating to criminal convictions and offences. More information about special category data and criminal conviction data is given in section 9 of this policy and in the Foundation's Appropriate Policy Document.

4. Scope and Responsibilities

This policy applies to all personal data processed by the Foundation, regardless of format (paper or electronic), and to all individuals who handle such data - including staff, Governors, volunteers, contractors, and third-party service providers.

Governors must ensure the Foundation complies with data protection law, oversees policy implementation, and promotes a culture of accountability.

All staff and Governors are required to comply with this policy. Breaches may result in disciplinary action. Accidental breaches may occur, but failure to report a breach that poses significant risk to individuals or the Foundation will be treated as a serious matter.

Contractors who process personal data on behalf of the Foundation are subject to binding contractual terms. Where contractors or volunteers act as independent Data Controllers, they are expected to comply with the same legal standards and best practices outlined in this policy.

When sharing personal data with third-party controllers (e.g. other schools, authorities, or parents/guardians), each party must have a lawful basis for processing and ensure appropriate security and confidentiality.

This policy is intended to support compliance with data protection law and does not override any statutory obligations, safeguarding duties, or legal requirements applicable to the Foundation.

5. Responsibility for Data Protection

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

The Foundation has appointed a Compliance Manager to lead on data protection matters. The Compliance Manager is responsible for overseeing compliance with this policy and applicable legislation, responding to data protection requests and enquiries, and liaising with external data compliance consultants as needed. 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:

- Handling personal data lawfully, fairly, and securely
- Collecting, storing, and processing personal data in accordance with this policy
- Seeking guidance from the Compliance Manager when unsure about data protection, retention, or security
- Reporting any concerns or suspected breaches of this policy without delay
- Consulting the Compliance Manager before starting any new activity that may involve personal data or affect individuals' privacy

Promoting a culture of data protection awareness and accountability across the Foundation

The Foundation has contracted Naomi Korn Associates (NKA) to provide external advisory support on data protection matters. While NKA offer expert guidance, they do not hold the statutory role of Data Protection Officer (DPO) for the Foundation.

Contractors and Employment Status

The Foundation engages a range of contractors and service providers who may process personal data on its behalf. Where contractors act as independent data controllers, they are expected to comply with the same legal standards and best practices outlined in this policy.

Contractors are encouraged to seek their own legal advice regarding their status and responsibilities under data protection law.

6. 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. **Lawfulness, Fairness and Transparency** – Personal data must be processed lawfully, fairly, and in a transparent manner.

2. **Purpose Limitation** – Data must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.

3. **Data Minimisation** – Data must be adequate, relevant, and limited to what is necessary.

4. **Accuracy** – Data must be accurate and kept up to date.

5. **Storage Limitation** – Data must not be kept for longer than necessary.

6. **Integrity and Confidentiality** – Data must be processed securely to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

In addition to these six principles, the UK GDPR includes a broader **accountability principle**, which requires Data Controllers to be able to demonstrate compliance with all the above principles. This includes maintaining records, conducting audits, and implementing appropriate policies and training.

7. 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.** Consent will be recorded securely and may be withdrawn at any time. The Foundation will maintain an audit trail of consent collection and withdrawal.

For further detail on which lawful basis applies to each category of data, see the Foundation's Privacy Notices.

Where special category data is processed, the Foundation also meets one of the additional conditions set out in the UK GDPR and the Data Protection Act 2018. More information is provided in section 9 of this policy and in the Foundation's Appropriate Policy Document.

The Foundation provides individuals with the information required by data protection law at the point of data collection.

The Foundation only collects personal data for specified, explicit and legitimate reasons and ensures that a lawful basis for processing is always in place. If personal data is to be used for a new purpose, individuals will be informed in advance, and consent will be sought where necessary.

8. Limitation, Minimisation and Accuracy

The Foundation takes all reasonable steps to ensure that personal data is not retained longer than necessary, in accordance with its Data Retention Policy. Data is securely destroyed as soon as it is no longer required, in accordance with the Foundation's Data Retention Policy.

In some cases, personal data may be retained for extended periods to comply with legal or regulatory obligations, or for legitimate organisational purposes (e.g. safeguarding, alumni relations, or historical archives).

The Foundation endeavours to ensure that all personal data is accurate, relevant, and up to date. Individuals are encouraged to inform the Foundation if they believe any personal data held about them is inaccurate or incomplete.

Where appropriate, individuals may have the right to request that inaccurate information is corrected or erased, depending on the nature of the data and the lawful basis for processing.

9. Processing of Special Category and Criminal Offence Data

As part of its statutory functions, the Foundation processes 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 Offence Data

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

Appropriate Policy Document

The Foundation is allowed to process this data under data protection law. 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. The APD sets out the procedures for ensuring compliance with the principles in Article 5 of the UK GDPR and outlines the Foundation's policies on retention and erasure.

The Foundation relies on the relevant conditions in Schedule 1 of the DPA 2018, including those relating to employment, safeguarding, equality of opportunity, and substantial public interest.

Additional special category processing

The Foundation also processes special category personal data in circumstances where an Appropriate Policy Document is not required. In all such cases, processing is carried out in accordance with the UK GDPR, respecting the rights and interests of data subjects. The lawful basis for processing is clearly explained in the Foundation's Privacy Notices.

10. Sharing Personal Data

10.1 General Principles

The Foundation shares personal data regularly as part of its educational, operational, pastoral, and safeguarding responsibilities. This includes sharing with other schools, service providers, exam boards, alumni networks, and external agencies, for example:

- Where there is a safeguarding concern involving a pupil or parent/guardian that may put the safety of Foundation staff or other pupils at risk
- When a pupil transfers to another school
- When organising a trip or event in collaboration with another school (e.g. an exchange programme)
- When liaising with external agencies (e.g. local authorities, health or safeguarding services); consent will be sought where appropriate, unless doing so would place an individual at risk
- Where suppliers or contractors require access to personal data to provide services to staff, pupils, or volunteers (e.g. IT providers, educational platforms, communication tools)

All data sharing must be lawful, proportionate, and documented. No new data sharing arrangement - whether internal, external, or involving third-party systems - may be initiated without prior written

approval from the Compliance Manager. This includes new platforms, services, informal exchanges, or any processing that differs from previously approved practices.

Staff must inform the Compliance Manager of any new or proposed data sharing so that:

- The lawful basis for processing can be established and documented.
- A Data Protection Impact Assessment (DPIA) can be conducted where necessary, particularly if the processing is likely to result in high risk to individuals.
- Any contracts or data sharing agreements with third parties can be reviewed to ensure appropriate safeguards are in place.
- Risks to data subjects - especially where special category data or children's data is involved—can be assessed and mitigated.
- Privacy notices can be updated and communicated to affected individuals, ensuring transparency and compliance.
- The Record of Data Processing can be updated.

Failure to follow these procedures may result in non-compliance with data protection legislation and could expose the Foundation to regulatory scrutiny or reputational harm.

10.2 Sharing with Suppliers and Contractors

When sharing data with suppliers or contractors, the Foundation will:

- Only appoint suppliers or contractors that provide sufficient guarantees of compliance with data protection law
- Establish a data sharing agreement, either within the contract or as a standalone agreement, to ensure lawful and fair processing
- Share only the minimum data necessary for the supplier or contractor to deliver their service and to ensure their safety while working with the Foundation

Where the Foundation engages sub-processors, it will ensure they are subject to prior written authorisation and bound by a written contract that meets the requirements of Article 28 of the UK GDPR.

Third-party processors are only permitted to process personal data on behalf of the Foundation for specified purposes and in accordance with documented instructions. They are not authorised to use personal data for their own purposes.

10.3 Use of Apps and Third-Party Services

Staff must not share personal or sensitive data with any app, software, or third-party service that has not been formally approved through the Foundation's third-party processor assessment process.

Even if a staff member consents to the use of their own personal data, the Foundation remains legally

responsible for ensuring that all data is processed securely and in compliance with data protection law.

Any requests to use a new app or service must be submitted for review. Personal data may only be shared once the app has passed the assessment and been formally approved.

10.4 Sharing with Law Enforcement and Government Bodies

The Foundation will share personal data with law enforcement agencies, regulators, or government bodies where legally required to do so. This includes, but is not limited to:

- The prevention or detection of crime or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- Compliance with legal proceedings
- Fulfilling safeguarding obligations
- Research and statistical purposes, provided the data is anonymised or consent has been obtained

10.5 Emergency Situations

Personal data may be shared with emergency services or local authorities where necessary to respond to an emergency involving a pupil, staff member, or volunteer.

10.6 International Data Transfers

Where personal data is transferred outside the UK or the European Economic Area (EEA), the Foundation will ensure that appropriate safeguards are in place. These may include:

- Adequacy decisions issued by the UK government
- Standard Contractual Clauses (SCCs)
- Other lawful transfer mechanisms in accordance with UK GDPR

Where personal data is transferred outside the UK or EEA, the Foundation will ensure appropriate safeguards are in place, such as Standard Contractual Clauses or adequacy decisions, in accordance with UK GDPR.

10.7 Sharing Educational Records

Under the UK GDPR and the Data Protection Act 2018, children may assume control of their personal data from the age of 13.

However, the Foundation may grant access to a pupil's educational records to their parents or guardians (including non-resident parents, unless legally restricted), in line with guidance from the Information Commissioner's Office (ICO), to support effective communication and engagement.

With appropriate consent, educational records may also be shared with other parties, such as grandparents.

Anonymised educational records may be shared with bursary donors to demonstrate the impact of their support.

11. Subject Access Requests

11.1 Overview of Subject Access Rights

Under the UK GDPR, individuals have a right to make a subject access request (SAR) to access personal data held about them by the Foundation. This includes:

- confirmation that their personal data is being processed
- access to a copy of the data
- the purposes of processing
- the categories of personal data concerned
- the recipients or categories of recipients that the data has been shared with or will be shared with
- the retention period, or the criteria used to determine it
- the source of the data, if not provided by the individual
- whether automated decision-making is applied and its significance or consequences.

11.2 How to Make a Subject Access Request

SARs must be submitted in writing to the Compliance Manager, either by letter or email at compliance@ksw.org.uk. Requests should include:

- the individual's full name
- correspondence address
- contact number and email address
- details of the information requested.

If a member of staff receives a SAR, they must forward it immediately to the Compliance Manager.

11.3 Requests on Behalf of Children

Personal data about a child belongs to the child, not the parent or guardian. A parent or guardian may make a SAR on behalf of their child only if:

- the child lacks the maturity to understand their rights; or
- the child has given consent

Children under 12 are generally not considered mature enough to understand their rights, so SARs from parents/guardians of Prep School pupils may be granted without the child's express permission. However, this is assessed on a case-by-case basis, with safeguarding considerations taken into account.

Where a pupil raises a concern confidentially and expressly withholds consent for disclosure to their parent/guardian, the Foundation will respect this unless it believes the pupil does not fully understand the implications, or disclosure is in the best interests of the pupil or others.

11.4 Responding to Subject Access Requests

When responding to SARs, the Foundation:

- may request two forms of identification
- may contact the individual by phone to confirm the request
- will respond without delay and within one month of verifying identity
- will provide the information free of charge
- may extend the response time to three months for complex or numerous requests, informing the individual within one month and explaining the reason

11.5 Grounds for Withholding Information

The Foundation may withhold information if disclosure:

- would cause serious harm to the physical or mental health of the data subject or another individual
- would reveal that a child is at risk of abuse, where disclosure is not in the child's best interests
- is contained in adoption or parental order records
- was provided in court proceedings concerning the child
- relates to examination scripts or marks not yet officially released
- is held in unstructured manual records not forming part of a filing system

If the request is unfounded or excessive (e.g. repetitive or requesting multiple copies), the Foundation may refuse to act or charge a reasonable administrative fee. The individual will be informed of the reason and their right to complain.

11.6 Third-Party Requests

SARs may be submitted by a third party on behalf of a data subject. In such cases:

- the third party must provide evidence of their authority (e.g. written consent or power of attorney)
- if no evidence is provided, the Foundation is not required to respond
- where possible, the Foundation will contact the data subject directly to confirm the request

11.7 Complaints and Escalation

If an individual is dissatisfied with the response to their SAR or believes their rights have not been upheld, they may raise a complaint. Please refer to the Foundation's Data Complaints Procedure.

Individuals also have the right to complain to the Information Commissioner's Office (ICO), but are encouraged to follow the Foundation's internal process first to allow concerns to be resolved promptly and fairly.

12. Other Rights of Individuals

In addition to the right to make a Subject Access Request (SAR), individuals have the following legal rights under the UK GDPR:

- To request that we correct inaccurate or incomplete personal data we hold about them
- To request the erasure of their personal data, where appropriate
- To request the restriction of processing of their personal data, in certain circumstances
- To receive their personal data in a commonly used, machine-readable format for transmission to another data controller ('data portability')
- To object to processing based on their particular situation, where they believe it has a disproportionate impact
- To object to automated decision-making, including profiling decisions are made without human involvement
- To object to the use of their personal data for direct marketing
- To request a copy of agreements under which their personal data is transferred outside of the UK or European Economic Area (EEA)
- To be notified of a personal data breach, where required by law
- To withdraw consent at any time, where consent is the lawful basis for processing
- To make a complaint to the Information Commissioner's Office (ICO) if they believe their data rights have been infringed.

Individuals should submit any request to exercise these rights to the Foundation's Compliance Manager at compliance@ksw.org.uk. If a member of staff receives such a request, they must immediately forward it to the Compliance Manager.

If an individual wishes to raise a concern or complaint about how their personal data has been handled, they are encouraged to follow the Foundation's Data Complaints Procedure, before contacting the ICO. This ensures the Foundation has the opportunity to resolve concerns promptly and fairly.

13. Biometric Recognition Systems

The Foundation does not collect, store, or otherwise process biometric data (e.g. fingerprints, facial recognition, or iris scans) for any purpose. Should this position change in the future, the Foundation will conduct a full data protection impact assessment and consult with stakeholders in accordance with the UK GDPR and the Protection of Freedoms Act 2012.

14. CCTV

The Foundation uses CCTV in various locations across its sites to help maintain a safe and secure environment for pupils, staff, volunteers, and visitors.

CCTV is used in accordance with the UK GDPR and the Data Protection Act 2018. The Foundation relies on the lawful basis of **legitimate interests** to operate CCTV systems, specifically for the purposes of safety, security, and safeguarding.

We follow the guidance issued by the Information Commissioner's Office (ICO) on the use of video surveillance and ensure that all CCTV systems are operated fairly, transparently, and for specified purposes.

Individuals are not required to give consent for CCTV use. However, we ensure that CCTV cameras are clearly visible and accompanied by prominent signage to inform individuals that recording is taking place.

The Foundation does not use CCTV for covert monitoring or to record sound, except in exceptional circumstances.

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

15. Photographic and Video Images

The Foundation may use photographs or video recordings of pupils for the following purposes:

- To hold a formal digital identity photograph of each pupil for pastoral and administrative purposes (not used for publicity).
- To record educational progress, achievement, and participation in co-curricular activities.

Use for Publicity and Marketing

Photographs and videos may be used for promotional or marketing purposes (e.g. on the Foundation's website, social media, newsletters, or printed materials) only where consent has been obtained from the individual or, where appropriate, the parent/guardian.

Where consent has been given, images may be used to support teaching and learning, celebrate pupil achievement, and promote the Foundation. Full names will not be published alongside images without the express written consent of the individual concerned or their parent/guardian, where appropriate.

Third-Party Media

The Foundation may allow third party media (e.g. journalists) to take photographs or video for journalistic purposes., Individual portrait images, whether captioned or not, will not be published by third party journalists without the express written consent of the relevant individual.

Where practicable, the Foundation will notify parents/guardians in advance when external media are expected to attend events involving pupils. Every reasonable effort will be made to ensure that pupils whose parents/guardians have refused permission are not photographed or filmed, and that such images are not shared with the media. The Foundation does not routinely provide full names of pupils to accompany media images.

Use Under Legitimate Interests

The Foundation may rely on legitimate interests to publish photographs and videos of Foundation events, including images of groups of parents/guardians, alumni or visitors. This includes uses that are reasonably expected within the school community, such as

- Inclusion in internal communications or printed materials (e.g. school magazines or the prospectus),
- Group images where individuals are not clearly identifiable.

Individuals may object to this type of processing, and any objections will be duly considered. The Foundation will not publish name-captioned individual portrait without express written consent.

Consent Management

On joining the Foundation, parents/guardians are invited to indicate their preferences regarding image

use via the Acceptance Form. Pupils in the Senior School are asked annually to provide consent for marketing-related image use.

Preferences may be amended at any time by writing to the Compliance Manager at compliance@ksw.org.uk. Changes will take effect from the date of written acknowledgement. Where consent is withdrawn, the Foundation will make reasonable efforts to prevent future user of the image, although it may not be possible to remove images already published or circulated.

Parental Photography

Parents/guardians and others may usually take photographs or video recordings at Foundation events (e.g. performances or sports fixtures) for personal, domestic use only. However, the Foundation does not permit the publication of images or photographs or videos of children other than your own, including on social media platforms such as Facebook, Instagram, or YouTube.

This policy reflects the Foundation's legal obligation to protect the privacy and, in some cases, the personal safety of pupils. It recognises that not all pupils or parents/guardians wish to have images or personal data published.

For further information, please refer to the Foundation's **Taking, Using and Storing Images of Children Policy**.

16. Artificial Intelligence (AI)

Artificial intelligence (AI) tools, including generative chatbots such as ChatGPT, Google Gemini, and Microsoft Copilot, are now widely accessible. The Foundation recognises the potential of these tools to support teaching, learning, and administrative efficiency, while also acknowledging the risks they pose to personal data, intellectual property, and academic integrity.

To protect personal and sensitive data, no individual is permitted to enter such data into unauthorised generative AI tools or chatbots. "Unauthorised" refers to any AI tool that has not been formally approved by the Foundation's IT or Compliance teams. Any breach of this rule will be treated as a data breach and managed in accordance with the Foundation's Data Breach Procedure.

Pupils retain intellectual property rights over original content they create. Their work must not be used to train generative AI models without their explicit consent. The Foundation does not permit the uploading of pupil work to AI platforms for training or analysis unless this has been specifically authorised and consent has been obtained.

The Foundation will continue to monitor developments in data protection law and emerging technologies, and will update this policy as necessary to reflect changes in regulation or best practice.

17. Data Protection by Design and Default

The Foundation integrates data protection into all data processing activities from the outset and throughout the lifecycle of any project. This approach ensures compliance with the UK GDPR's principles of data minimisation, purpose limitation, and accountability.

Measures in place include:

- Appointing a suitably experienced Compliance Manager and ensuring they have the necessary resources and training to fulfil their duties
- Retaining the services of a qualified external data compliance consultant
- Only processing personal data that is necessary for each specific purpose, in line with the data protection principles outlined in Section 6
- Completing Data Protection Impact Assessments (DPIAs) where processing data presents a high risk to individuals' rights and freedoms, or when introducing new technologies
- Embedding data protection into internal documents, including this policy, related policies, and privacy notices
- Providing regular training to staff on data protection law and maintaining completion records Conducting regular reviews and audits to test our privacy measures and ensure compliance
- Maintaining records of processing activities, including:
    - Contact details of the Compliance Manager and information required to share with data subjects (via Privacy Notices)
    - Internal records of the type of data, data subjects, purposes, recipients, storage methods, retention periods, and security measures.

Data Protection Impact Assessments (DPIAs)

A DPIA is a process to help identify and minimise the data protection risks in any project involving personal data. The Foundation completes DPIAs for:

- Any processing likely to result in a high risk to individuals
- Major projects involving new technologies
- Processing involving vulnerable groups, including children.

DPIAs are completed before processing begins and include:

- A description of the nature, scope, context, and purpose of processing
- An assessment of necessity, proportionality, and compliance
- An evaluation of risks to individuals
- Measures to mitigate those risks

The level of risk is assessed based on both the likelihood and severity of potential harm. Where a high risk cannot be mitigated, the Foundation will consult the Information Commissioner's Office (ICO) before proceeding.

DPIA outcomes are integrated into policies, procedures, and operational practice.

18. Data Security and Storage of Records

The Foundation protects personal data and ensures it is safeguarded against unlawful access, alteration, processing or disclosure, as well as accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records containing personal data are kept under lock and key when not in use
- Confidential documents must not be left on desks, staffroom tables, noticeboards, or in other accessible areas
- When personal data needs to be taken off-site, staff must follow the relevant procedures and ensure all records are returned to school promptly.
- Passwords used to access Foundation devices must be 12 characters long and include letters, numbers and special characters. Staff and pupils are reminded to update passwords regularly
- Encryption software is used to protect all portable devices and removable media (e.g. laptops, USB drives)
- Staff, pupils, and Governors who store personal data on personal devices must follow the same security procedures as for Foundation-owned equipment
- When sharing personal data with third parties, the Foundation conducts due diligence and ensures appropriate safeguards are in place.

Email accounts and inboxes must be used for communication only and not as a long-term storage solution for personal data.

The Foundation's archive is maintained as a resource to help inspire and inform current pupils and staff, celebrate the heritage of the Foundation, and support research into the history of the school and its community. Archived materials are managed in accordance with the Foundation's Data Protection and Data Retention Policies to ensure the continued protection of personal data.

19. Disposal of Records

Personal data that is no longer required will be securely disposed of in accordance with data protection legislation. Data that is inaccurate or out of date will also be securely destroyed, unless it is retained in our Foundation archive as described in section 18.

Secure disposal methods include shredding or incineration of paper records, and deletion or overwriting of electronic files. Where disposal is carried out by a third party, appropriate contractual safeguards will be in place to ensure compliance with data protection requirements.

Further details are provided in the Foundation's Data Retention Policy.

20. Personal Data Breaches

The Foundation takes appropriate measures to minimise the risk of personal data breaches. In the event of a suspected breach, the procedure outlined in the Foundation's Data Breach Procedure will be followed.

Where required, the breach will be reported to the Information Commissioner's Office (ICO) within 72 hours of discovery. Examples of personal data breaches in an educational context may include, but are not limited to:

- Publication of a non-anonymised dataset on the Foundation website showing exam results of pupils eligible for the pupil premium
- Disclosure of safeguarding information to an unauthorised individual
- Theft of a Foundation-owned laptop containing unencrypted personal data about pupils

High-risk breaches may result in regulatory action, including financial penalties. It is therefore essential that all staff remain vigilant and report any concerns immediately in accordance with internal procedures.

21. Training

All staff and Governors receive data protection training as part of their induction. Ongoing training will be provided as part of continuing professional development, particularly when there are changes to legislation, regulatory guidance, or internal processes that affect data protection responsibilities.

22. Processing of Credit Card Data

The Foundation adheres to the requirements of the Payment Card Industry Data Security Standard (PCI DSS) when handling credit card information. Staff responsible for processing such data must ensure they are familiar with, and comply with, the most current PCI DSS requirements.

Other categories of financial and identity-related information—such as bank account details, salary information, national insurance numbers, and passport details—may not be classified as legally sensitive under data protection law. However, due to the potential impact on individuals if misused, such data must be handled with a high level of care and in accordance with the Foundation's data protection procedures.

23. Complaints

Queries or complaints regarding personal data or this policy should be directed to the Foundation's Compliance Manager:

Email: compliance@ksw.org.uk

Telephone: 01905 721700

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

Complaints Process:

- All complaints will be acknowledged within **30 calendar days**.
- The Foundation will investigate the matter and provide updates throughout the process.
- A written outcome will be provided, including any actions taken.
- If you are dissatisfied with the outcome, you may escalate your complaint to the **Information Commissioner's Office (ICO)**.

The Foundation maintains a record of all complaints in accordance with its data retention policy.

For further information, please refer to the Foundation's **Data Complaints Procedure**

24. Related Policies

- Privacy Notices
- Acceptable Use Policies
- Safeguarding Policy
- Behaviour Management Policy
- Staff Code of Conduct
- Governors' Code of Conduct
- CCTV Policy
- Data Breach Procedure
- Data Retention Policy
- Appropriate Policy Document
- Data Complaints Procedure
- Taking, Storing and Using Images of Children Policy

25. Version Control

Version No	Date	Summary of changes	Changes made by
1	03/02/2025	Minor changes to policy	Liz Sydenham, Compliance Manager
2	07/10/2025	Significant update to policy, including addition of Version Control tracking.	Liz Sydenham, Compliance Manager

26. Approval

The Governing Body will review and approve significant policy changes, especially those affecting data subject rights, lawful bases for processing and data sharing or retention practices.

Version #	Approval Date	Approval Confirmed by
1	28 March 2025	Pat Preston, Chair of Governors
2	5 December 2025	Pat Preston, Chair of Governors