King's Worcester

Data Protection Policy

Effective 1st September 2026

Contents

1. Introduction 3
2. Accessibility Statement 3
3. Definitions 4
4. Scope 5
5. Responsibilities for Data Protection 5
6. Data Protection Principles 6
7. Lawfulness, Fairness and Transparency 6
8. Data Minimisation and Accuracy 7
9. Processing of Special Category and Criminal Offence Data 7
10. Sharing Personal Data 9
11. Subject Access Requests 11
12. Other Rights of Individuals 13
13. Biometric Recognition Systems 14
14. CCTV 14
15. Photographic and Video Images 15
16. Audio and Video Recording 16
17. Artificial Intelligence (AI) 17
18. Digital Monitoring and Filtering 18
19. Data Protection by Design and Default 18
20. Data Security and Storage of Records 19
21. Processing of Credit Card Data 20
22. Retention and Disposal of Records 20
23. Personal Data Breaches 20
24. Training 21
25. Complaints 21
26. Related Policies 21
27. 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.

The Foundation has regard to relevant guidance issued by the Department for Education (DfE), the Information Commissioner's Office (ICO), and other relevant regulatory, statutory or sector bodies when developing its data protection policies, practices and procedures.

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. 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.

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

This policy applies to all personal data processed by the Foundation, regardless of format (paper or electronic), and to all staff, Governors, and volunteers who handle such data in the course of their work or duties.

Third parties (including contractors such as peripatetic music teachers) who process personal data on behalf of the Foundation are subject to appropriate contractual obligations and must comply with data protection law. Where third parties act as independent Data Controllers, they are responsible for ensuring their own compliance with data protection legislation.

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.

Any questions about the operation of this policy or any concerns that it has not been followed should be referred in the first instance to the Compliance Manager via compliance@ksw.org.uk.

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

5. Responsibilities for Data Protection

The Governing Body has overall responsibility for ensuring that the Foundation complies with all relevant data protection obligations and for promoting a culture of accountability across the organisation.

The Foundation has appointed a Compliance Manager to lead on data protection matters. This includes overseeing compliance with this policy and applicable legislation, advising staff on data protection requirements, and coordinating responses to data protection requests and enquiries.

All staff, Governors and volunteers are required to comply with this policy and with applicable data protection law. Breaches may result in disciplinary action. While accidental breaches may occur, any failure to report a known or suspected breach that poses a risk to individuals or to the Foundation will be treated as a serious matter.

All staff, Governors and volunteers are responsible for:

- handling personal data lawfully, fairly, and securely
- collecting, storing, and processing personal data in accordance with this policy
- seeking guidance when unsure about data protection, retention, or security requirements
- reporting any concerns or suspected breaches 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 considered whether it is required to appoint a Data Protection Officer (DPO) under UK GDPR and has determined that this is not necessary, having regard to the nature, scope, context, and purposes of its data processing activities. This position will be kept under review in light of regulatory and sector guidance.

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

The Foundation processes personal data in accordance with the principles of lawfulness, fairness, and transparency under UK GDPR. This means that all personal data must be processed on a valid lawful basis, in a way that individuals would reasonably expect, and with clear information provided about how their data is used.

7.1 Lawful Basis for Processing

The Foundation relies on the following lawful bases when processing personal data:

- **Contract** – where processing is necessary to fulfil a contract with the individual, or to take steps at their request before entering into a contract (e.g. educating a pupil or employing a member of staff)
- **Legal Obligation** – where processing is necessary for the Foundation to comply with a legal requirement (e.g. safeguarding duties, regulatory reporting, employment law obligations)
- **Vital Interests** – where processing is necessary to protect someone's life or prevent serious harm (e.g. sharing medical information in an emergency)
- **Legitimate Interests** – where processing is necessary for the Foundation's legitimate interests or

those of a third party, provided these are not overridden by the rights and freedoms of the individual (e.g. routine school administration, pastoral care, and safeguarding)

- **Consent** – where the individual (or their parent/guardian, where appropriate) has given clear, informed 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.
- The 'public task' lawful basis is not generally relied upon by the Foundation, as it primarily applies to public authorities exercising statutory functions.

Further detail on the lawful basis applicable to specific types of processing is set out in the Foundation's Privacy Notices.

7.2 Special Category Data

Where the Foundation processes special category or criminal offence data, it will also identify and document an additional condition for processing, in accordance with the UK GDPR and the Data Protection Act 2018. Further information is provided in Section 9 and in the Foundation's Appropriate Policy Document.

7.3 Transparency and Fair Processing

The Foundation provides individuals with clear and accessible information about how their personal data is used, typically through Privacy Notices issued at the point of data collection.

Personal data is only collected for specified, explicit, and legitimate purposes. It will not be used for purposes that are incompatible with those originally communicated, unless a new lawful basis is identified and individuals are informed in advance. Where required, consent will be obtained before any new processing takes place.

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. Data Minimisation and Accuracy

The Foundation aims to ensure that personal data is adequate, relevant and limited to what is necessary for the purposes for which it is processed.

The Foundation also takes reasonable steps to ensure personal data is accurate and kept up to date. Individuals are encouraged to notify the Foundation of inaccuracies so that records may be corrected where appropriate.

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.

9.1 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 an individual
- data concerning health; or
- data concerning a natural person's sex life or sexual orientation.

9.2 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'.

9.3 Appropriate Policy Document

The Foundation processes special category and criminal offence data only where it has identified an appropriate lawful basis and condition for processing under the UK GDPR and the Data Protection Act 2018.

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.

9.4 Additional special category processing

The Foundation may process 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.

9.5 Safeguarding and Criminal Offence Information

Special category and criminal offence data may arise in connection with safeguarding, child protection, welfare and disciplinary matters involving pupils, staff or members of the wider Foundation community. Such information is processed only where necessary and proportionate in accordance with statutory responsibilities and applicable data protection legislation.

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, welfare or legal reason to do so
- 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.

However, the Foundation recognises that effective safeguarding depends on the timely and appropriate sharing of information. Where concerns exist regarding the safety or welfare of a child, personal data may be shared without consent where there is a lawful basis to do so and where it is necessary to protect the vital interests of a child or fulfil safeguarding obligations.

Staff should never allow data protection concerns to prevent appropriate sharing of safeguarding information.

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

10.7 Sharing Educational Records

Under the UK GDPR and the Data Protection Act 2018, children aged 13 and over are generally considered capable of exercising their own data protection rights. 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.

10.8 Safeguarding Records

Safeguarding records are kept separately from the main pupil file and access restricted to authorised safeguarding staff.

Where a pupil transfers to another school or educational setting, safeguarding information will be transferred securely, promptly and with appropriate audit records. The Foundation will verify the identity of the receiving organisation before any transfer takes place.

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 Receipt of a Subject Access Request

A Subject Access Request (SAR) can be made in writing, verbally, or through any other communication channel, and does not need to refer to data protection legislation to be valid. Any request from an individual asking for access to their personal data should be treated as a SAR.

All staff must treat any such request seriously and must not attempt to respond directly. Any SAR received must be forwarded immediately to the Compliance Manager at compliance@ksw.org.uk.

Staff must treat any request for personal data as time-sensitive and act without delay. The statutory timeframe for responding to a SAR begins when the request is received by the Foundation.

Upon receipt of a SAR, staff must:

- forward the request without delay
- preserve all relevant information and records, including emails, messages, and notes
- not delete, amend, or alter any records that may fall within the scope of the request

Failure to follow these requirements may result in non-compliance with data protection law and may be treated as a disciplinary matter.

The Compliance Manager will coordinate the response to all SARs and will provide further instructions as required.

Staff may be required to conduct reasonable searches of systems, email accounts, and records when instructed.

11.3 How to Make a Subject Access Request

Subject Access Requests may be made in writing, verbally, or by any other means. Individuals are encouraged to submit requests in writing to the Compliance Manager...

Requests should include:

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

11.4 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.

11.5 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

11.6 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.

11.7 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

11.8 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.

The Foundation recognises that recording technologies may also be present in privately owned devices, including smart glasses, mobile phones, wearable cameras and other connected devices. Unauthorised recording may constitute a safeguarding concern, disciplinary matter or personal data breach.

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.

15.1 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.

15.2 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.

15.3 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.

15.4 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 use of the image,

although it may not be possible to remove images already published or circulated.

15.5 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.

15.6 Emerging Risks of Image Misuse

The Foundation recognises the rapidly evolving risks associated with emerging technologies, including the misuse of personal data such as pupil images (for example, through manipulation, synthetic media, or "deepfake" technologies).

The Foundation will continue to monitor developments in this area and will review its practices and policies to ensure that appropriate safeguards are in place. Where relevant, the Foundation will have regard to guidance issued by regulatory bodies, sector organisations, and safeguarding authorities, and will take proportionate steps to protect pupils, staff, and the wider school community from harm.

16. Audio and Video Recording

16.1 Audio and Video Recording

The recording of meetings, lessons, or conversations (including audio or video recordings) must be appropriate, proportionate, and supported by a clear lawful basis for processing under UK GDPR. Recordings should only take place where there is a legitimate need to do so.

All participants must be clearly informed where recording is taking place, including the purpose of the recording and how it will be used. Recordings constitute personal data where individuals can be identified and must be processed fairly, lawfully and transparently in accordance with this policy and the Foundation's safeguarding and monitoring requirements.

Where recordings contain personal data, they may be disclosable to individuals in response to a Subject Access Request or other data rights request under UK GDPR. Staff should be aware that recordings may be reviewed, disclosed, or relied upon in decision-making processes.

All recordings must be handled, stored, and retained securely in accordance with the Foundation's Data Protection and Data Retention Policies. Unauthorised or inappropriate recording may be treated as a disciplinary matter.

Parents, pupils, and visitors are not permitted to make audio or video recordings of meetings, lessons, or conversations involving other individuals without the knowledge and consent of those involved, except where there is a lawful reason for doing so. The Foundation reserves the right to restrict or prohibit recording on its premises or at its events in order to protect the privacy, safety, and wellbeing of pupils and staff.

16.2 Wearable Technology

The Foundation recognises that wearable technologies, including smart glasses, AI-enabled devices, smart watches and similar products, may have the capability to capture, store, transmit or analyse personal data, including images, video and audio recordings.

Staff, pupils, governors, volunteers and visitors must not use wearable devices to record individuals within the Foundation community without appropriate authorisation and a lawful basis for doing so.

The use of wearable technologies must comply with the Foundation's safeguarding, data protection, acceptable use and staff conduct policies.

Any concerns regarding the misuse of wearable technologies should be reported immediately to the Compliance Manager and, where relevant, the Designated Safeguarding Lead.

17. Artificial Intelligence (AI)

17.1 Use of Artificial Intelligence

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.

17.2 Personal Data and AI Tools

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.

17.3 Intellectual Property and Pupil Work

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.

17.4 Staff Responsibilities

Use of AI tools must comply with the Staff Acceptable Use Policy and may be monitored. Staff must not rely solely on AI-generated outputs where these may impact individuals, and must review and verify accuracy before use or retention.

17.5 Deepfakes

The Foundation recognises that artificial intelligence technologies can create realistic but fabricated images, audio recordings and videos ("deepfakes"). Such content may present safeguarding, welfare and reputational risks.

Any AI-generated content involving pupils, staff or members of the wider Foundation community must be treated as a potential safeguarding concern and reported in accordance with safeguarding procedures.

18. Digital Monitoring and Filtering

The Foundation uses filtering, monitoring and security technologies to assist in identifying safeguarding concerns, misuse of technology and threats to the security of Foundation systems.

Such systems may process personal data relating to users of Foundation networks and devices.

Monitoring is carried out proportionately, transparently and in accordance with applicable legislation and Foundation policies.

19. Data Protection by Design and Default

The Foundation integrates data protection into all data processing activities from the outset and throughout the lifecycle of projects, systems and services. This approach helps ensure compliance with the UK GDPR principles of lawfulness, transparency, data minimisation, purpose limitation, storage limitation, integrity and confidentiality, and accountability.

19.1 Implementation

The Foundation implements data protection by design and default through the following measures:

- Appointing a suitably experienced Compliance Manager and ensuring they have the resources and training necessary to fulfil their responsibilities
- Processing only the 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 is likely to present 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 data protection training to staff and Governors and maintaining appropriate training records
- Conducting regular reviews and audits to test our privacy measures and ensure compliance
- Maintaining a Record of Processing Activities (RoPA).

19.2 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.

19.3 Access Management

Access to personal data is restricted to individuals who require access in order to fulfil their role.

The Foundation:

- applies role-based access controls wherever practicable;
- reviews access permissions periodically;
- removes or amends access promptly when staff, governors, volunteers, contractors or other authorised users change roles or leave the Foundation;
- implements multi-factor authentication where appropriate;
- maintains audit logs where available; and
- applies other technical and organisational measures necessary to protect personal information.

Special category data, safeguarding records and other sensitive information are subject to enhanced access controls and may only be accessed by authorised personnel with a legitimate business, legal or safeguarding need.

19.4 Children's Data

The Foundation recognises that children merit specific protection in relation to their personal data. When selecting, implementing or reviewing online services, educational technology platforms, monitoring systems, or AI-enabled systems that may be accessed by pupils, the Foundation will have regard to the Information Commissioner's Office (ICO) Age Appropriate Design Code (Children's Code).

The Foundation will assess risks to children's rights and freedoms through appropriate due diligence and, where required, Data Protection Impact Assessments (DPIAs). Particular consideration will be given to transparency, profiling, geolocation, data sharing, behavioural monitoring, targeted advertising, and the use of personal data in ways that may not be in a child's best interests.

20. 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.

21. 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.

22. Retention and Disposal of Records

Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected and in accordance with the Foundation's Data Retention Policy. Retention periods take account of legal, regulatory, safeguarding and operational requirements.

In some circumstances, records may be retained for historical, archival or research purposes where this is lawful and appropriate. The Foundation maintains an archive to preserve its history and heritage and support research into the life of the school and its community. Archived materials are managed in accordance with the Foundation's Data Protection and Data Retention Policies.

Records which have reached the end of their retention period will be securely disposed of in accordance with the Data Retention Policy.

23. 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
- Unauthorised access to safeguarding records or systems.
- 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.

24. Training

All staff, Governors and volunteers 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.

25. 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**

26. 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 Protection Complaints Procedure
- Taking, Storing and Using Images of Children Policy

27. 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.