THE KING'S SCHOOL

GRANTHAM

The Data Protection Policy

Contents

1 Aims

1.1 This is the Data Protection policy of The King's School (**Academy**).

1.2 The school as the Data Controller will comply with its obligations under the UK General Data Protection Regulation and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 (**GDPR)** and (**DPA)**. The school is committed to being concise, clear and transparent about how it obtains and uses personal data and will ensure data subjects are aware of their rights under the legislation.

2 Scope and application

2.1 This policy applies to the whole Academy.

2.2 This policy applies to all members of the Academy community, including staff and volunteers and pupils.

2.3 personal data is defined in the Glossary.

2.4 The School collects a large amount of personal data every year, including pupil records, staff records, names and addresses of those requesting information, examination marks, references, fee collection, as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with the statutory obligations of Local Authorities (LAs), government agencies and other bodies.

3 Regulatory framework

3.1 This policy has been prepared to meet the Academy's responsibilities under:

3.1.1 Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) as amended by the Data (Use and Access) Act 2025;

3.1.2 Equality Act 2010.

3.2 This policy has regard to the following guidance and advice:

3.2.1 Keeping Children Safe in Education (DfE, September 2024)

3.3 The following Academy policies, procedures and resource materials are relevant to this policy:

3.3.1 Safeguarding and Child Protection Policy and Procedures;

3.3.2 Behaviour Policy;

3.3.3 Risk Assessment Policy for Pupil Welfare;

3.3.4 Staff Code of Conduct and Whistleblowing Policy;

3.3.5 The Online Safety Policy

4 Publication and availability

4.1 This policy is published on the Academy website.

4.2 This policy is available in hard copy on request.

4.3 A copy of the policy is available for inspection from the PA to the Head during the school day.

4.4 This policy is available on the school's SharePoint Site.

5 Definitions

5.1 Where the following words or phrases are used in this policy:

5.1.1 References to the **Proprietor** are references to the King's School, the (**Academy Trust**).

6 Responsibility statement and allocation of tasks

6.1 The Proprietor has overall responsibility for all matters which are the subject of this policy.

Task	Allocated to	When / frequency of review
Keeping the policy up to date and compliant with the law and best practice	The School Business Leader	As a minimum annually, ideally termly, and as required
Monitoring the implementation of the policy (including the record of incidents involving the use of technology and the logs of internet activity and sites visited), relevant risk assessments and any action taken in response and evaluating the effectiveness	The School Business Leader	As a minimum annually, ideally termly, and as required
Maintaining up-to-date records of all information created in relation to the policy and its implementation as required by the UK GDPR	The School Business Leader	As required, and at least termly
Formal annual review	Proprietor	As a minimum annually, and as required
Overall responsibility for content and implementation	Proprietor	As a minimum annually

7 The Principles

7.1 The principles set out in the GDPR must be adhered to when processing personal data:

7.1.1 Personal data must be processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)

7.1.2 Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)

7.1.3 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (data minimisation)

7.1.4 Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (accuracy).

7.1.5 Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (storage limitation)

7.1.6 Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal data is processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or

unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (integrity and confidentiality).

7.1.7 The school, as Data Controller, shall be responsible for and able to demonstrate compliance with all of the principles set out above (accountability). This includes maintaining appropriate documentation of processing activities, implementing suitable technical and organisational measures, training staff, conducting Data Protection Impact Assessments where required, and appointing a Data Protection Officer. The school will keep records sufficient to demonstrate its compliance and will make these available to the Information Commissioner's Office on request

8 Transfer Limitation

8.1 Personal data shall not be transferred to a country or territory outside the United Kingdom unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data, as determined by the UK Secretary of State by way of an adequacy regulation, or where the organisation receiving the data has provided appropriate safeguards in accordance with the UK GDPR and the Data Protection Act 2018. Where no adequacy regulation is in place, transfers may only proceed on the basis of a lawful transfer mechanism, such as International Data Transfer Agreements (IDTAs) or the UK Addendum to standard contractual clauses, as approved by the Information Commissioner's Office.

9 Lawful Basis for processing personal data

9.1 Before any processing activity starts for the first time, and then regularly afterwards, the Data Protection Officer (or relevant staff member) must identify the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

9.1.1 Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school.

9.1.2 Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract.

9.1.3 Processing is necessary for compliance with a legal obligation to which the data controller is subject.

9.1.4 Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

9.1.5 Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party.

9.1.6 The data subject has given consent to processing his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters.

9.1.7 Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

9.2 When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school's public tasks) a legitimate interest's assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

10 Sensitive Personal data

10.1 Processing of sensitive personal data (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified.

10.2 Sensitive personal data is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

10.3 Sensitive personal data will only be processed if:

10.3.1 There is a lawful basis for doing so as identified.

10.3.2 One of the special conditions for processing sensitive personal data applies:

(a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent

(d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim

(e) the processing relates to personal data, which are manifestly made public by the data subject

(f) the processing is necessary for the establishment, exercise or defence of legal claims

(g) the processing is necessary for reasons of substantial public interest

(h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services

(i) the processing is necessary for reasons of public interest in the area of public health.

10.4 The school's privacy notice(s), available on the school's website, set out the types of sensitive personal data that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

10.5 Sensitive personal data will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

11 Automated Decision Making

11.1 Where the school carries out automated decision-making (including profiling), it must meet all the principles and have a lawful basis for the processing. Explicit consent will usually be required for automated decision-making (unless it is authorised by law or necessary for performing or entering into a contract).

Data subjects have a right under Article 22 of UK GDPR to request a human review of any automated decisions.

12 Data Protection Impact Assessments (DPIA)

12.1 The School's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

12.2 Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

12.2.1 whether the processing is necessary and proportionate in relation to its purpose

12.2.2 the risks to individuals

12.2.3 what measures can be put in place to address those risks and protect personal data.

12.3 When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

13 Documentation and records

13.1 Written records of processing activities must be kept and recorded including:

13.1.1 the name(s) and details of individuals or roles that carry out the processing

13.1.2 the purposes of the processing

13.1.3 a description of the categories of individuals and categories of personal data

13.1.4 categories of recipients of personal data

13.1.5 details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

13.1.6 retention schedules

13.1.7 a description of technical and organisational security measures.

13.2 As part of the School's record of processing activities the DPO will document, or link to documentation on:

13.2.1 Information required for privacy notices.

13.2.2 Records of consent.

13.2.3 Controller-processor contracts.

13.2.4 The location of personal data.

13.2.5 DPIA.

13.2.6 Records of data breaches.

13.3 Records of processing of sensitive information are kept on:

13.3.1 The relevant purposes for which the processing takes place, including why it is necessary for that purpose.

13.3.2 The lawful basis for our processing.

13.3.3 Whether the personal data is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

13.4 The School should conduct regular reviews of the personal data it processes and update its documentation accordingly. This may include:

13.4.1 Carrying out information audits to find out what personal data is held.

13.4.2 Talking to staff about their processing activities.

13.4.3 Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

14 Privacy Notice

14.1 The school publishes its Privacy Notice on the school's website, The King's School Grantham - Data Privacy Notices, informing data subjects about the personal data that we collect and holds relating to individual data subjects, how individuals can expect their personal data to be used and for what purposes.

15 Purpose Limitation

15.1 Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

16 Data Minimisation

16.1 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

16.2 Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

16.3 The School maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

17 Individual Rights

17.1 Staff as well as any other 'data subjects' have the following rights in relation to their personal data:

17.1.1 To be informed about how, why and on what basis that information is processed (see the relevant privacy notice).

17.1.2 To obtain confirmation that personal data is being processed and to obtain access to it and certain other information, by making a subject access request.

17.1.3 To have data corrected if it is inaccurate or incomplete.

17.1.4 To have data erased if it is no longer necessary for the purpose for which it was originally collected, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten').

17.1.5 To restrict the processing of personal data where the accuracy of the information is contested, or the processing is unlawful (but the individual does not want the data to be erased) or where the school no longer need the personal data, but the individual requires the data to establish, exercise or defend a legal claim.

17.1.6 To restrict the processing of personal data temporarily where the individual does not think it is accurate (and the school are verifying whether it is accurate), or where the individual has objected to the processing (and the school are considering whether the school's legitimate grounds override their interests).

17.1.7 In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

17.1.8 To withdraw consent to processing at any time (if applicable).

17.1.9 To request a copy of an agreement under which personal data is transferred outside of the EEA.

17.1.10 To object to decisions based solely on automated processing, including profiling.

17.1.11 To be notified of a data breach which is likely to result in high risk to their rights and freedoms.

17.1.12 To make a complaint to the Information Commissioner's Office (ICO) or a Court.

Individual Responsibilities

17.2 During their employment, staff may have access to the personal data of other members of staff, suppliers, clients or the public. The school expects staff to help meet its data protection obligations to those individuals.

17.3 If you have access to personal data, you must:

17.3.1 only access the personal data that you have authority to access and only for authorised purposes

17.3.2 only allow other staff to access personal data if they have appropriate authorisation

17.3.3 only allow individuals who are not school staff to access personal data if you have specific authority to do so

17.3.4 keep personal data secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies)

17.3.5 not remove personal data, or devices containing personal data (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device

17.3.6 not store personal data on local drives or on personal devices that are used for work purposes

18 Information Security

18.1 The school will use appropriate technical and organisational measures to keep personal data secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

18.2 All staff are responsible for keeping information secure in accordance with the legislation and must follow the school's acceptable usage policy.

18.3 The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

18.4 Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

18.5 Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction.

18.6 Staff must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

18.6.1 Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

18.6.2 Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

18.6.3 Availability means that authorised users can access the personal data when they need it for authorised purposes.

18.7 Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA.

18.8 Where the school uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. Contracts with external organisations must provide that:

18.8.1 the organisation may only act on the written instructions of the school

18.8.2 those processing data are subject to the duty of confidence

18.8.3 appropriate measures are taken to ensure the security of processing

18.8.4 sub-contractors are only engaged with the prior consent of the school and under a written contract

18.8.5 the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection

18.8.6 the organisation will delete or return all personal data to the school as requested at the end of the contract

18.8.7 the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

18.9 Before any new agreement involving the processing of personal data by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

19 Storage and retention of personal data

19.1 Personal data will be kept securely in accordance with the school's data protection obligations.

19.2 Personal data that is no longer required will be deleted in accordance with the Schools Record Retention Schedule.

20 Data breaches

20.1 A data breach may take many different forms:

20.1.1 Loss or theft of data or equipment on which personal data is stored

20.1.2 Unauthorised access to or use of personal data either by a member of staff or third party

20.1.3 Loss of data resulting from an equipment or systems (including hardware or software) failure

20.1.4 Human error, such as accidental deletion or alteration of data

20.1.5 Unforeseen circumstances, such as a fire or flood

20.1.6 Deliberate attacks on IT systems, such as hacking, viruses or phishing scams

20.1.7 Blagging offences where information is obtained by deceiving the organisation which holds it

20.2 The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

20.3 Staff should ensure they inform their line manager, the DPO or the Head immediately that a data breach is discovered and make all reasonable efforts to recover the information.

21 Consequences of a failure to comply

21.1 The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal data is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

21.2 Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

21.3 If you have any questions or concerns about this policy, you should contact the DPO.

22 The Supervisory Authority in the UK

22.1 Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

23 Version control

Date of adoption of this policy	May 2012
Date of last review of this policy	May 2026
Date for next review of this policy	June 2027

24 Glossary

Automated Decision-Making (ADM)

When a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

Automated Processing

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. profiling is an example of automated processing.

Consent

Agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

Data Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The school is the Data Controller of all personal data relating to its pupils, parents and staff.

Data Subject

A living identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA)

Tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

Data Protection Officer (DPO)

The person required to be appointed in public authorities under the GDPR.

Explicit Consent

Consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR)

General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the GDPR.

Personal data

Any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data breach

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

Privacy by Design

Implementing appropriate technical and organisational measures in an effective manner to ensure compliance.

Privacy Notices

Separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing

Anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

Processor

Natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Pseudonymisation or Pseudonymised

Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data

Information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.