KING JAMES I ACADEMY

Data Protection Policy (GDPR)

Date adopted by Governors: March 2020

Date of Next Review: March 2022

General Data Protection Regulation

1. Aims & Objectives

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- the law regarding personal data
- how personal data should be processed, stored, archived and disposed of
- the rights in respect of people whose data is being held and processed by the school (this includes pupils, parents, staff and governors).

1.1 Safeguarding

The Data Protection Act 2018 and GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children.

Keeping children safe in Education
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

1.2 It is a statutory requirement for all schools to have a Data Protection Policy:

http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools

In addition to this policy, schools should have:

- Retention Information - details on how long all records are retained
- Information Asset Audit - a comprehensive audit listing all the information that the school holds, who has access to the information and the legal basis for processing it
- Privacy Notices - for pupils, parents, staff and governors
- Registered with the ICO

This policy will link with the following:

- Safeguarding Policy
- Staff AUP/Code of Conduct
- Photographic Policy
- Photographic Consent Forms

1.3 Definitions

- Personal Data - information relating to a living individual, who can be identified directly from that data or indirectly by reference to other data held. (Note that

information can be in any form - written, on a PC e.g. names, addresses, photos.)

- Data Processor – a person who handles the data including filing or storing it.
- Data Subject – the person about whom personal data is processed or kept.
- Data Controller - the person or organisation who determines the “how and what” of data processing in an organisation.

1.4 Data Protection Principles

Article 5 of the GDPR sets out that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to measures respecting the principle of ‘data minimisation’, not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and again subject to the ‘data minimisation’ principle; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2 Lawful Basis for Processing Data

GDPR stipulates that there must be a lawful basis for processing data, and that for special category data an additional condition has to be met. The vast majority of information that schools collect and process is required to enable the school to perform

tasks carried out in the public interest or in the exercise of official authority vested in the school, as the data controller.

2.1 Age

Children under the age of 13 are not usually considered able to give consent to process data or to directly access the rights of a data subject, so parents or guardians can do this on their behalf, providing this is in the best interests of the child. See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/

2.2 Consent

If there is a lawful basis for collecting data, then consent to collect data is not required. (An employee could not opt to withhold an NI number for example.) However, a privacy notice which explains to data subjects (or the parents of the data subject if under the age of 13) will be required. This explains the lawful basis for processing the data, and also explains to the individual their rights.

Parents/Carers or children over the age of 13 will need to give consent when there is not a legal reason for processing, for instance for images used in school publicity or social media feeds. The consent will be transparent, revocable, and will need to be on an "Opt-in" basis.

3 RIGHTS

GDPR provides the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Different rights attach to different lawful bases of processing:

	Right to erasure	**Right to portability**	**Right to object**
Vital Interests	✓	**X**	**X**
Legal Obligation	**X**	**X**	**X**
Public Task	**X**	**X**	✓
Legitimate Interests	✓	**X**	✓

Contract	✓	✓	**X**
Consent	✓	✓	**X** but right to withdraw consent

3.2 The right to be informed – *See Privacy Notices section 6.2*

3.3 The right of access

Depending on the age of the pupil, there are two legal basis for pupils or parents to request access to their data – a Subject Access Request or a request under the 2005 Education Regulations.

3.3.1 Subject Access request under GDPR

GDPR gives individuals the right to access any data that an organisation holds on them. This will be completed within 30 days without charge.

Further guidance is available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Guidance from the ICO highlights the rights of the child. Before responding to a subject access request for information held about a child, The Academy will consider whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights, then we will respond directly to the child. However, we may allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

3.3.2 In maintained schools, parents have another statutory right to access their children's educational record

This is part of the Education (Pupil Information) Regulations 2005. This applies to all children under 16 years and has to be completed in 15 working days. See https://ico.org.uk/your-data-matters/schools/pupils-info/

3.3.3 Information which may be withheld

On some occasions records could contain information which ***"is likely to cause significant harm to the physical or mental health of the child or others",*** for instance, if a child makes a disclosure of abuse. In these circumstances, the data will not be released and the pupil/parent does not need to be informed of its existence.

3.4 The right to erasure

GDPR includes a right to erasure – but this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data.

It will be seen from the table above that, where a school relies on either a 'legal obligation' or a 'public task' basis for processing (see section 3), there is no right to erasure – however, this does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or the school's data retention guidelines.

4 Data Types

- Personal Data

  The Academy has access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances.

  This will include:

  - Personal information about members of the school community – including students, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records
  - Curricular/academic data e.g. class lists, pupil/student progress records, reports, references
  - Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references
  - Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

- Special Category Data

  "Special Category Data" are data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a person's health or sexual life is prohibited except in special circumstances.

  Special category data is more sensitive, and so needs more protection.

  In a school the most likely special category data is likely to be:

  - information on the racial or ethnic origin of a pupil or member of staff
  - information about the sexuality of a child, his or her family or a member of staff
  - medical information about a child or member of staff (SEND)
  - (some information regarding safeguarding will also fall into this category)

- staffing e.g. Staff Trade Union details.

- Other types of Data not covered by the act

  This is data that does not identify a living individual and, therefore, is not covered by the remit of the DPA - this may fall under other 'access to information' procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources and other information about the school which does not relate to an individual. Some of this data would be available publicly (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (if the school has written a detailed scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

5 Responsibilities

The Headteacher and Governing Body are responsible for Data Protection; they should appoint a Data Protection Officer to manage data.

5.1 Risk Management – Roles: *Data Protection Officer*

The school should have a nominated member of staff responsible for the management of data protection.

According to the ICO the minimum role will include:

- to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

  Other staff within the Academy have been delegated responsibility for particular issues, for instance the handling of SEND information.

5.2 Risk management - Staff and Governors Responsibilities

Everyone in the school has the responsibility of handling personal information in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

6 Legal Requirements

6.1 Registration

The Academy must be registered as a Data Controller on the Data Protection Register held by the Information Commissioner. The register may be checked by visiting https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/

6.2 Information for Data Subjects (Parents, Staff): PRIVACY NOTICES

In order to comply with the fair processing requirements of the DPA, the Academy must inform parents/carers of all pupils/students and staff of the data they collect, process and hold on the pupils/students, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. LA, DfE, etc) to whom it may be passed.

Privacy notices are available to pupils, parents and carers via the school website. A paper copy will be enclosed within the admission pack when children first register for school.

7 Transporting, Storing and Disposing of personal Data

7.1 Information security - Storage and Access to Data

The more sensitive the data the more robust the security measures will need to be in place to protect it.

7.1.1 Technical Requirements

The Academy will ensure that IT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.

The Academy has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

7.1.2 Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

7.1.3 Passwords

All users will use strong passwords (8 Characters including a Capital letter, number and symbol) which must be updated occasionally. User passwords must never be shared.

7.1.4 Images

Images will be protected and stored in a secure area. See school Photographic Policy.

7.1.5 Cloud Based Storage

The Academy has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Google Apps and Onedrive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The Academy will ensure that it is satisfied with controls put in place by remote/cloud based data services providers to protect the data.

7.2 Third Party data transfers

As a Data Controller, the Academy is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party, as well as data processing agreements.

7.3 Retention of Data

The guidance given by the Information and Records Management Society is used as a basis for determining how long records are kept. This Academy's retention information is available to data subjects on request.

Personal data that is no longer required will be destroyed and this process will be recorded.

7.4 Systems to protect data

7.4.1 Paper Based Systems

All paper based personal data will be protected by appropriate controls, for example:

- paper based safeguarding chronologies will be in a locked cupboard when not in use
- class lists used for the purpose of marking may be stored in a teacher's bag.

- Paper based personal information sent to parents will be checked before the envelope is sealed.

7.4.2 School Websites

Uploads to the school website will be checked prior to publication, for instance:

- to check that appropriate photographic consent has been obtained
- to check that the correct documents have been uploaded.

7.4.3 E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

All internal Academy email addresses are automatically encrypted.

Where technically possible, all external e-mail containing sensitive information will be encrypted by attaching the sensitive information as a word document and encrypting the document or by using the security features available in Office 365.

8 Data Sharing

8.1 Sharing with the LA and DfE

The Academy is required by law to share information with the LA and DfE. Further details are available at: https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

8.2 Safeguarding

Schools MUST follow the statutory processes in Keeping Children safe in Education and Working together to Safeguard Children
https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

Durham LSCB provides information on information sharing at: http://www.durham-lscb.org.uk/wp-content/uploads/sites/29/2016/06/Guide-for-professionals-on-information-sharing.pdf

8.3 Transfer of Safeguarding and SEND records when a pupil moves school

The following is an extract from keeping Children safe in Education Sept 2019.

- Where children leave the school or college, the designated safeguarding lead should ensure their child protection file is transferred to the new school or college as soon as possible, ensuring secure transit, and confirmation of receipt should be obtained. For schools, this should be transferred separately from the main pupil file.

- Receiving schools and colleges should ensure key staff such as designated safeguarding leads and SENCOs or the named person with oversight for SEN in a college, are aware as required.

- In addition to the child protection file, the designated safeguarding lead should also consider if it would be appropriate to share any information with the new school or college in advance of a child leaving. For example, information that would allow the new school or college to continue supporting victims of abuse and have that support in place for when the child arrives.

9 Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

- In the event of a data breach, the data protection officer will inform the Headteacher and Chair of Governors.
- When a personal data breach has occurred, the Academy must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, the Academy must notify the ICO; if it's unlikely the Academy does not have to report it. However, if the Academy decide not to report the breach, it needs to be able to justify this decision, and it should be documented.
- The Academy must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If the Academy takes longer than this, it must give reasons for the delay.
- If a breach is likely to result in a high risk to the rights and freedoms of individuals, GDPR states the Academy must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.

Any report about a data breach must include:

- a description of the nature of the personal data breach including, where possible:

    - the categories and approximate number of individuals concerned; *and*
    - the categories and approximate number of personal data records concerned;

- the name and contact details of the data protection officer or other contact point where more information can be obtained;

- a description of the likely consequences of the personal data breach; *and*
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach including, where appropriate, the measures taken to mitigate any possible adverse effects.

Further details are available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Our Commitment:

King James I Academy is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).
https://ico.org.uk/for-organisations/guide-to-data-protection/data-protectionprinciples/

The Academy is committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

Notification:

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO:
https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data:

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions/
The principles of the Data Protection Act (GDPR) shall be applied to all data processed:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes

- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation. https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency-and-control/

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authority, DfE etc. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed

Data Retention:
We will only retain the data we collect for as long as is necessary. This would be to satisfy the purpose for which it has been collected in accordance with our data retention policy.

Personal data that is no longer required will be destroyed and the process will be recorded.

Data Security:
In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

Simon Whitehead
Acting Headteacher
King James I Academy
South Church Road
Bishop Auckland
DL14 7JZ

No charge will be applied to process the request.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools**
  If a pupil transfers from King James I Academy to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- **Examination authorities**
  This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

- **Health authorities**
  As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**
  If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- **Social workers and support agencies**
  In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Educational division**
  Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

- **Right to be Forgotten:**
  Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.

It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard.

Electronic data, records, and personal information are stored on the Staff Shared Area, and is only accessible by named individuals.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances

- Unwanted paper copies of data, sensitive information or pupil files should be placed in the secure bins around the site. This also applies to handwritten notes if the notes reference any other staff member or pupil by name
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers
- All fixed devices e.g. Desktop computers must be password protected. Passwords should have a mixture of lowercase text, capital letters and numbers
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended
- Sensitive information should not be viewed on public computers
- If it is necessary to transport data away from the school, it should be downloaded onto an encrypted USB stick which will be provided by the Academy. The data should not be transferred from this stick onto any home or public computers
- Work should be transferred to the schools hard drive from the encrypted USB on the next working day and the work on the encrypted USB deleted
- USB sticks used by staff to transport personal or sensitive data must be encrypted. These are available on request from Karen Sams
- All portable devices such as laptops and memory sticks must be encrypted
- Media data should be transferred to the schools hard drive from portable devices on the next working day then deleted
- Personal data should not be stored on any piece of equipment that is not owned by the school

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

The Academy uses only qualified sources for disposal of IT assets and collections. The Academy also uses the Shred Centre to dispose of sensitive data that is no longer required.

Data Breach Procedures:

Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately the Data Protection Officer will:

- Inform the Headteacher and Chair of Governors
- Follow procedures set out in the Data Protection Policy Potential Breach Procedure

Policy Review Reviewing:

This policy will be reviewed, and updated if necessary every two years or when legislation changes.

Date: Review date

Signed:
Chair of Governors

Adopted by the Governing Body on _____

The Data Protection Officer is: Karen Sams