King's Group Academies
Data Protection Policy

Date adopted: 4 December 2018 by KGA Trustees
Date Reviewed: 10 December 2019
Date of review: Annually

Contents:

1. About This Policy

Everyone has rights with regard to the way in which their personal data is handled. During the course of the Academy's activities it collects, stores and processes personal data about staff, pupils, their parents, suppliers and other third parties, and it is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

Those who are involved in the processing of personal data are obliged to comply with this Policy when doing so. Any breach of this Policy may result in disciplinary action.

This Policy sets out the basis on which the Academy will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. It does not form part of any employee's contract of employment and may be amended at any time.

The policy meets the requirements and expectations of the General Data Protection Register introduced in law as of the 25th May 2018.

2. General Statement of Duties

The Academy is required to process relevant personal data regarding individuals as part of its operation and shall take all reasonable steps to do so in accordance with this Policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data.

3. Data Protection Officer

Each Academy must appoint a Data Protection Officer(DPO), who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the Act. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the DPO. Details of the DPO can be found on the school website.

4. The Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice as enshrined within the requirements of the GDPR.

These provide that personal data must be:

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

5. Types of Personal Data Processed by the Academy

Personal data covers both facts and opinions about an individual. The Academy may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including, by way of example:

- Names, addresses, telephone numbers, email addresses and other contact details
- Bank details and other financial information, e.g. about parents who pay fees to the Academy
- Past, present and prospective pupils' academic, disciplinary, admissions and attendance
- records (including information about any special needs), and examination scripts and marks
- Where appropriate, information about individuals' health, and contact details for their next of kin
- References given or received by the Academy about pupils, and information provided by
- previous educational establishments and/or other professionals or organisations working with pupils

- Images of pupils (and occasionally other individuals) engaging in Academy activities, and images captured by the Academy's CCTV system (in accordance with the Academy's policy on taking, storing and using images of children)

Generally, the Academy receives personal data from the individual directly (or, in the case of pupils, from parents). However, in some cases personal data may be supplied by third parties (for example, another Academy, or other professionals or authorities working with that individual), or collected from publicly available resources

6. Sensitive Personal Data

The Academy may, from time to time, need to process sensitive personal data regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act and will only be processed by the Academy with the explicit consent of the appropriate individual, or as otherwise permitted by the Act. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the DPO for more information on obtaining consent to process sensitive personal data.

7. Use of Personal Data by the Academy

The Academy will use (and where appropriate share with third parties) personal data about individuals for a number of purposes as part of its operations, including as follows:

- For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents
- To provide education services (including SEN), career services, and extra-curricular activities to pupils; monitoring pupils' progress and educational needs; and maintaining relationships with alumni and the Academy community
- For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the Academy's performance;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil has attended or where it is proposed they attend
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the Academy
- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of Academy trips;
- To monitor (as appropriate) use of the Academy's IT and communications systems in accordance with the Academy's Computing and Acceptable Use and E-safety Policies
- To make use of photographic images of pupils in Academy publications, on the Academy website and (where appropriate) on the Academy's social media channels in accordance with the Academy's policy on taking, storing and using images of children
- For security purposes, and for regulatory and legal purposes (for example safeguarding and child protection and health and safety) and to comply with its legal obligations; and

- Where otherwise reasonably necessary for the Academy's purposes, including to obtain appropriate professional advice and insurance for the Academy

8. Keeping in Touch and Supporting the Academy

The Academy will use the contact details of parents, alumni and other members of the Academy community to keep them updated about the activities of the Academy, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the Academy may also:

- Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the Academy community, (e.g. PTA to be determined)
- Contact parents and/or alumni (including PTA – to be determined) by post and email in order to promote and raise funds for the Academy and, where appropriate, other worthy causes
- Should you wish to limit or object to any such use, or would like further information about them, please contact the DPO in writing.

9. Rights of Access to Personal Data ('Subject Access Request')

Individuals have the right under the Act to access to personal data about them held by the Academy, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the DPO. The Academy will endeavour to respond to any such written requests as soon as is reasonably practicable and, in any event, within statutory time limits (one month).

It should be noted that certain data is exempt from the right of access under the Act. This may include information which identifies other individuals or information which is subject to legal professional privilege. The Academy is also not required to disclose any pupil examination scripts (though examiners' comments may be disclosed), nor any reference given by the Academy for the purposes of the education, training or employment of any individual.

The GDPR states that pupils under the age of 16 are to be considered as 'vulnerable' and therefore are not allowed to amend their own data. All subject access requests from pupils will therefore not be considered until such time as we have a sixth form or advice changes.

Only a person with parental responsibility will generally be expected to make a subject access request on behalf of younger pupils. A pupil of any age may ask a parent or other representative to make a subject access request on their behalf. In line with the GDPR, we recognise the following rights in relation to data:

a) **Right of Access** - Individuals have the right to obtain confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to that personal data.
b) **Right to Rectification** - Individuals have the right to obtain rectification of inaccurate personal data and the right to provide additional personal data to complete any incomplete personal data.
c) **Right to Erasure ("Right to be Forgotten")** - In certain cases, individuals have the right to obtain the erasure of their personal data.
d) **Right to Restriction of Processing** - Individuals have the right to obtain a restriction of processing, applicable for a certain period and/or for certain situations.

e) **Right to Data Portability** - Individuals have the right to receive their personal data and they have the right to transmit such personal data to another controller.
f) **Right to Object** - In certain cases, individuals have the right to object to processing of their personal data, including with regards to profiling. They have the right to object at further processing of their personal data in so far as they have been collected for direct marketing purposes.
g) **Right to be Not Subject to Automated Individual Decision-Making** - Individuals have the right to not be subject to a decision based solely on automated processing.
h) **Right to Filing Complaints** - Individuals have the right to file complaints about the processing of their personal data with the relevant data protection authorities.
i) **Right to Compensation of Damages** - In case of a breach of the applicable legislation on processing of (their) personal data, individuals have the right to claim damages that such a breach may have caused with them.

10. Exemptions

Certain data is exempted from the provisions of the Act, including the following:

- The prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Academy
- Information which might cause serious harm to the physical or mental health of the pupil or another individual
- Cases where the disclosure would reveal a child is at risk of abuse
- Information contained in adoption and parental order records
- Information given to a court in proceedings under the Magistrates' Courts (Children and Young Persons) Rules 1992
- Copies of examination scripts; and
- Providing examination marks before they are officially announced

11. Unstructured Personal Information

The Academy will generally not be required to provide access to information held mutually and in an unstructured way.

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the DPO.

Further exemptions may include information which identifies other individuals, information which the Academy reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The Academy will also treat as confidential any reference given by the Academy for the purpose of the education, training or employment, or prospective education, training or employment of any pupil. The Academy acknowledges that an individual may have the right to access a reference relating to them received by the Academy. However, such a reference will only be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent or if disclosure is reasonable in all the circumstances.

12. Whose Rights?

The rights under the Act are those of the individual to whom the data relate. However, the Academy will, in most cases rely on parental consent to process data relating to pupils (if consent is required under the Act) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent.

Parents should be aware that in such situations they may not be consulted.

In general, the Academy will assume that pupils consent to disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the Academy's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the Academy will maintain confidentiality unless, in the academy's opinion, there is a good reason to do otherwise; for example, where the Academy believes disclosure will be in the best interests of the pupil or other pupils.

Pupils are required to respect the personal data and privacy of others, and to comply with the Academy's Computing and Acceptable Use and E-safety Policies and any Academy rules.

13. Disclosure of Information

The Academy may receive requests from third parties to disclose personal data it holds about pupils, their parents or guardians. The Academy confirms that it will not generally disclose information unless the individual has given their consent or one of the specific exemptions under the Act applies. However, the Academy does intend to disclose such data as is necessary to third parties for the following purposes:

- To give a confidential reference relating to a pupil to any educational institution which it is proposed that the pupil may attend
- To give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend
- To publish the results of public examinations or other achievements of pupils of the Academy
- To disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of Academy trips

Where the Academy receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure.

14. Accuracy

The Academy will endeavour to ensure that all personal data held in relation to an individual is as up-to-date and accurate as possible. Individuals must notify the DPO of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the DPO in writing.

15. Timely Processing

Except as required by the Independent Inquiry into Child Sexual Abuse (see below) the Academy will not keep personal data longer than is necessary for the purpose or purposes for which they were collected and will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required.

16. Enforcement

If an individual believes that the Academy has not complied with this Policy or acted otherwise than in accordance with the Act, they should utilise the Academy's complaints procedure and should also notify the DPO.

17. Data Security

The Academy will take appropriate technical and organisational steps to ensure the security of personal data about individuals, and to ensure that members of staff will only have access to personal data relating to pupils, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this policy and their duties under the Act.

The Academy must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of or damage to, personal data. Accordingly, no member of staff is permitted to remove personal data from Academy premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar. Where a member of staff is permitted to take data offsite it must be encrypted.

The Independent Inquiry into Child Sexual Abuse

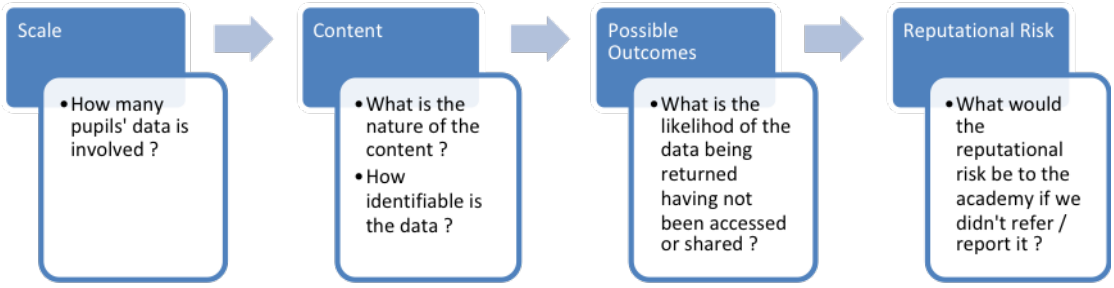
The Independent Inquiry into Child Sexual Abuse (formerly The Goddard Inquiry) was launched at the beginning of July 2015. The Inquiry is investigating whether public bodies and other non-state institutions have taken seriously their duty of care to protect children from sexual abuse in England and Wales. Judge Goddard made it very clear in her opening statement the importance of retaining records. She wrote to institutions including local authorities and religious organisations on the subject of retaining records but confirmed that the content of those letters should be taken to apply to all institutions which have had responsibility for the care of children.

In view of Judge Goddard's clear direction to institutions not to destroy records, the Academy will not destroy pupil records after the customary seven-year period, as determined by the DPO in accordance with the Data Protection Principles published by the Information Commissioner's Office but will retain them and all staff records until the Inquiry has concluded. The Inquiry 'trumps' any data protection legislation.

18. Data Breaches

The academy takes seriously any data breach and will, through its policy and practice endeavour to minimise the risk of a breach. However, in the rare circumstances surrounding a data breach a process will be followed. This process can be seen in Appendix A.

The GDPR states that breaches should be referred to the Information Commissioners Office (ICO) within 72 hours of disclosure. However, it is appropriate for our academy to consider the following factors before referring to the ICO:



19. Complaints

Complaints related to the management of data in our academy will be handled through our existing Complaints Procedure, copies of which are available on the academy website or from the academy office upon request.

20. Requests for Amendments of Data

The GDPR establishes the right to amend any data held that is inaccurate or may have a negative or detrimental effect on an individual. Amendments may take the form of updates, redactions or removals. As an academy, we believe that before any amendment request is granted the first step is to view the data so as to ensure that it may be necessary. However, in the rare circumstances surrounding a data amendment request a process will be followed. This process can be seen in Appendix B.

21. Transparency and Accountability

To ensure that the academy is open and transparent about what data it holds and how it will be managed, the academy will bear in mind the following prompts in all that it does:

The academy will provide every parent with information in relation to their data rights. In addition, it will also provide every new parent with a data statement. This 'statement' will outline the aspects of data that the academy will gather and use, as well as stating their purpose, their 'shelf-life' and where it may be shared. Parents will be asked to acknowledge their understanding of this information and accept the reasoning and processing that may occur.

22. Academy Website

The academy will establish a page on its website to ensure that its approaches, policies and practices in relation to data are transparent. It will provide parents with information that may be relevant to their data concerns. It will include:

- Information about the academy's Data Protection Officer (name, contact details etc)
- Copies of relevant policies
- Data review and amendment request forms
- Process flowcharts
- Step by step guides
- Complaints policy

23. Introducing A New Initiative or Project

The GDPR requires academies to undertake an evaluation of the data management impact resulting from new initiatives. As an academy we will undertake this using our proforma which can be found in Appendix C.

24. The Academy's Rights to Refuse a Request

The academy reserves the right to refuse a request to view or amend data held. This would be rare and only on the following basis:

- Vexatious requests
- Where information held maybe required by future legal processes e.g. Child Protection
- The request would lead to inaccurate and misleading information being recorded
- The request has come from an individual who has no rights of access

Where the academy decides not to adhere to a request it will notify the person who requested of:

- The reason why the request has been refused
- Their legal rights of appeal or complaint
- Their legal rights of referral to the ICO

25. Charges

The academy will not usually make a charge in relation to data viewing or amendment requests. However, it reserves the right to do so where the request is proven to be:

- Vexatious
- Excessive
- Unfounded

26. Generic Policies

The academy will undertake to review all of its policies (curriculum, safety, statutory etc) to ensure that any potential data management issues are identified and resolved. The review statement will accompany the relevant document.

27. Transitional Period

The introduction of the GDPR has required the academy to undertake a significant review of policy and practice in relation to data. Throughout the implementation period, from May 2018 to August 2019, we will keep the implementation under regular review. This will be undertaken by: e.g.

- Annual Data Protection Audits
- Annual Reports to Governors by the Academy's DPO
- An Annual Data Statement

Appendices: (now attached)
A: Data Breach Process Flowchart
B: Data Amendment Request Process Flowchart
C: New Initiative Impact Assessment Proforma

28. Management of policy

The King's Group Academies Trustees has overall responsibility for the maintenance and operation of this policy. They will maintain a record of concerns raised and the outcomes. King's Group Academies policies will be reviewed regularly and will include an evaluation for impact on workload and working hours.

Appendix A
Data Breach Process

When discovered, a breach will be logged on GDPRiS: https://app.gdpr.school/login and will be reported to the Head of School/ Executive Principal.

The decision whether to report the breach to the ICO or the data subject (or their parents/carers) will based on the criteria in clause 18, taking into account the reporting requirements, ie that a breach should be reported to the ICO if it is likely to present a risk to the rights and freedoms of the individual, and to be reported to the data subject if it is likely to present a *high* risk of harm to their rights and freedoms. The Trust's Data Protection Officer (Sue Collins) can help to make this decision.

The circumstances surrounding the breach will be investigated by or on behalf of the Head of School/Executive Principal, and measures put in place to prevent a recurrence. Any advice or instructions received from the ICO will be actioned.

All actions will be logged on GDPRiS, and the breach marked as closed once the Head of School/Executive Principal (or ICO if appropriate) is satisfied.

Appendix B
Data Amendment Request

Some data held on students, parents and staff is routinely checked and updated as necessary, for instance staff addresses on the payroll system or contact details for students and their parents, which parents are invited to keep up to date on a regular basis. However, if students or parents request a change to data which is not routinely updated they will be asked to complete the following form and to present it with proof of identification.

The applicant will be issued with a receipt for the form.

The Academy will investigate the request and if necessary seek evidence that the data held is incorrect. A reply will be sent to the applicant within one calendar month, stating whether or not the request is accepted. If it is, the amendments will be made immediately. If not, the applicant will be advised of the reasons.

Data Amendment Request Form

Academy Name	
Student's Details	
Name	
Date of Birth	
Current Address	
Current Class	
Person Requesting Data Amendment	
Name	
Relationship to the Student	
Address	
Telephone Number	
Do you have parental responsibility?	
Your Request	
What data/which records do you wish to have amended?	
What amendment do you want? Do you want the data to be updated, amended or deleted?	
Why do you want these changes made?	

Please sign this request …

Signed _____ Date _____

Once completed, please hand this form to the Academy Office, who will ensure that it is passed to the correct person. You will be issued with a receipt for it. We are required to respond to your request within one calendar month of receipt of this form.

NB: Should your request be accepted we would not normally make a charge. However, we reserve the legal right to do so if your request is vexatious, excessive or unfounded.

Appendix C
New Initiative Impact Assessment Pro Forma (also called Data Protection Impact Assessment – DPIA)

This template is provided by the Information Commissioner's Office (ICO) as an example of how to record DPIA process and outcome. It follows the process set out in the ICO DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The template may be adapted to suit the complexity of the project. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons

Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA