KADER ACADEMY

DATA PROTECTION POLICY

KADER ACADEMY

DATA PROTECTION POLICY

Date reviewed	Approved by
Spring 2015	Staffing and Resources Committee
10th February 2016	Finance and Resource Committee
14th February 2017	Finance and Resource Committee
23rd April 2018	Finance and Resource Committee
27th April 2020	Finance and Resources Committee
22nd March 2021	Full Governing Body

CONTENTS

1. Introduction

The Academy aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information (CCTV).

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number i.e. unique pupil reference number (UPN), employee no. • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and requires more protection, including information about an individual's: • Racial or ethnic origin

	• Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, sharing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

Kader Academy processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The academy is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

The Data Protection policy applies to all staff employed by Kader Academy, and to external organisations or individuals working on behalf of the academy. Staff who do not comply with this policy may face disciplinary action.

The Governing Body of Kader Academy Trust has overall responsibility for ensuring that the Academy complies with all relevant data protection obligations.

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing body and, where relevant, advise the governing body on academy data protection issues.

The Data Protection Officer is the first point of contact for individuals whose data is processed by the academy, and also the first point of contact for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

The Data Protection Officer for Kader Academy Trust is Caroline Finn who can be contacted via the school office or by emailing; School.Enquiries@kaderacademy.org.uk

The Principal acts as the representative of the Data Controller on a day to day basis.

All Staff are responsible for;

- Collecting, storing and processing all personal data in accordance with this policy.
- Informing the academy of any changes to their personal data, such as change of name or address.
- Contacting the Data Protection Officer in the following circumstances;
    1. With any questions relating to the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    2. If they are concerned that the policy is not being adhered to.
    3. If they are unsure as to whether or not they have a lawful basis to use personal data in a particular way.
    4. If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside of the European Economic Area.
    5. If there has been a data breach.

6. Before they engage in an activity which may affect the privacy rights of an individual.
7. If they need help with contracts or will be sharing data with third parties.

6. Data Protection Principles

The General Data Protection Regulation (GDPR) is based on data protection principles which the academy must comply with.

The principles state that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

The Data Protection policy sets out how the academy aims to comply with these principles.

7. Collecting Personal Data

Lawfulness, fairness and transparency

The academy will only process personal data where it has at least one of the following six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the academy can **fulfil a contract** with the individual, or the individual has asked the academy to take specific steps before entering into a contract.
- The data needs to be processed so that the academy can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
- The data needs to be processed so that the academy, as a public authority, can perform a task **in the public interest,** and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the academy or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

For special categories of personal data, the academy must also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Where the academy offers online services to pupils, such as classroom apps, and it intends to rely on consent as a basis for processing, parental consent will be obtained in the form of a signed 'Acceptable use of computers and the internet agreement'.

Whenever the academy first collects personal data directly from individuals, it will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy

The academy will only collect personal data for specified, explicit and legitimate reasons. These reasons will be explained to the individuals when the academy first collects their data.

Should the academy wish to use personal data for reasons other than those given when it was first obtained, the individual concerned will be informed prior to doing so and consent will be sought where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the academy's records management policy.

8. Sharing Personal Data

The academy will not normally share personal data with anyone else, but may do so if:

- There is an issue with a pupil or parent/carer that puts the safety of academy staff at risk.
- The academy needs to liaise with other agencies – consent will be sought, as necessary, before doing this.
- Suppliers or contractors need data to enable the academy to provide services to staff and pupils – for example, the academy's IT support and/or HR providers. When doing this the academy will:
    - Only appoint suppliers or contractors who are able to provide sufficient guarantees that they comply with data protection law.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.

- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the academy.

The academy will also share personal data with law enforcement and government bodies where it is legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy the academy's safeguarding obligations.
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

The academy may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects pupils or staff.

Should the academy be required to transfer personal data to a country or territory outside of the European Economic Area, it will be done so in accordance with data protection law.

9. Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the academy holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include the following details:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers' of pupils of the academy may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, the academy:

- May ask the individual to provide two forms of identification.
- May contact the individual via telephone to confirm that the request was made.
- Will respond without delay and within one month of receipt of the request.
- Will provide the information free of charge.
- May inform the individual that the academy will comply within three months of receipt of the request, where a request is complex or numerous. The academy will inform the individual of this within one month, and explain why the extension is necessary.

The academy will not disclose information if it:

- May cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, the academy may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When the academy refuses a request, the individual will be informed of the reason why, and they will be informed that they have the right to complain to the ICO.

Additional data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when the academy is collecting their data about how it is used and processed (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Request that the academy rectifies, erases or restricts processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement which might negatively affect them).
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.

- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If a member of staff receives such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.
This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

The academy uses CCTV in various locations around the school site to ensure it remains safe. The academy adheres to the ICO's code of practice for the use of CCTV.

Individuals' permission to use CCTV is not required, however, the academy makes it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Mrs. C. Finn (School Business Manager).

12. Photographs and videos

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. On occasion the media is invited into the academy to take photographs, film footage or video recordings which would then be available to the wider community. As part of daily school activities, the academy may take photographs and record images of individuals within the school.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. The academy will comply with the Data Protection Act and request parents/carers permission before taking images of members of the academy.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking site, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Consent can be refused or withdrawn at any time. If consent is withdrawn, the academy will delete the photograph or video and not distribute it further.

When using photographs and videos in this way the academy will not include personal information about the child, to ensure they cannot be identified.

13. Data protection by design and default

Kader Academy will put measures in place to show that integrated data protection has been incorporated into all data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing privacy impact assessments where the academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; a record of attendance will be kept.
- Regularly conducting reviews and audits to test privacy measures and ensure compliance.

- Maintaining records of processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the academy and DPO and all information which it shares about how their personal data is processed and used (via privacy notices)
    - For all personal data which the academy holds, maintaining an internal record of the type of data, data subject, how and why data is being used, any third-party recipients, how and why the academy stores the data, retention periods and how the data is being kept secure

14. Data security and storage of records

The academy will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the school office.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- When emailing data of a sensitive nature which includes pupil information i.e. names, addresses dates of birth etc. Staff must always password protect documents and send the password via a separate email.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (refer to the academy's acceptable use policy).

Where there is a requirement to share personal data with a third party, the academy carries out due diligence and takes reasonable steps to ensure it is stored securely and is adequately protected.

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where the academy cannot or does not need to rectify or update it.

For example, paper-based records will be shredded and electronic files will be deleted. The academy may also use a third party to safely dispose of records on the school's behalf, for example ONE IT (the academy's IT provider). All third parties must provide sufficient guarantees that disposal complies with data protection law.

16. Personal data breaches

The academy will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the procedures set out in appendix 1 will be followed.

Any data breach will be reported to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised data set being published on the school website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft or loss of a school laptop containing non-encrypted personal data about pupils.

17. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and shared with the governing body annually.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Principal and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will consider whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions will be stored securely on the electronic office drive within the Data Protection folder.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all of the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored securely on the electronic office file within the Data Protection folder.
- The DPO and Principal will meet to review what happened and establish ways in which it could be prevented from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

The academy will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The effectiveness of these actions will be reviewed and amended as necessary after any data breach.

Actions which will be taken by the academy for breaches of risky or sensitive personal data include:

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT Provider (One IT) to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure that the academy receives a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, the academy will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

Other types of breach to consider include:

- *Non-anonymised pupil exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*