KEYS Academy Trust

Data Protection Policy

Updated for GDPR/Data Protection Act 2018

KEYS Academy Trust
Unlocking the future

Version control summary and overview details

TKAT Statutory Policy • All schools require a policy on this area. • There should be no changes to the core text. • LGBs will minute that they have noted Trust approval and will adopt the policy effective immediately. • This is a Trust policy to be implemented by all schools within The Keys Academy Trust to ensure a consistent approach for all.
Version control • 1.3 Updated DPO contact details and school responsibilities • 3.2 Addition of wording "where appropriate, criminal data will be processed in line with Article 10 of the UK GDPR and schedule 1 of DPA 2018" • Change of Data Protection Officer to Data Protection Lead. • Additions and amendments to sections 3.3d, 3.3.1, 4.2, 5.1b, 5.2b, 5.4, 6.4, 7.3, 10.1-10.6 • Amends to Appendix A point 5 and Appendix B, point 7

Reviewed by (Trust Officer)	Hester Wooller, CEO
Approved by TKAT Trustee Committee:	FAPPP
Trust date of approval:	June 2026
Trust date of next review:	June 2027

TKAT vision
We are a family of distinctive schools at the heart of the diverse communities we serve. In line with our Christian ethos, we aspire to excellent learning and pastoral care for pupils and staff and are committed to being open and welcoming to all.

Key areas of note
Please note the following, which will be applicable throughout the policy:

- Any reference to 'headteacher' should read as whatever title is relevant to the school using the policy (i.e. Executive Headteacher/Head of School or Headteacher). Anything else will be explicitly referenced within the policy.
- Any reference to 'everyone' to staff, trustees, local governors and pupils.
- Any reference to 'we' should be read as The Keys Academy Trust.
- Any reference to 'parents' should be read as 'parents, carers and guardians'.

KEYS Academy Trust
Unlocking the future

Table of Contents

1. Introduction 4
2. Legislation and guidance 4
3. Data protection principles and categories of data 4
4. Roles and responsibilities 5
5. Data Protection documentation 6
6. Freedom of Information Act (FOI) 7
7. Security and storage 7
8. Retention and disposal 7
9. Training 8
10. Complaints 8

Appendix A: Data breach information and procedures 9
Appendix B: Subject Access Request (SAR) process and timescales 10
Appendix C: Freedom of Information (FOI) process and timescales 11
Appendix D: Document Retention and Disposal Schedule 12

1. Introduction

1.1 Our school is committed to protecting all data that it holds relating to staff, pupils, parents and governors.

1.2 This policy applies to all school data, regardless of whether it is in paper or electronic format and where it is stored.

1.3 The Data Protection Officer (DPO) for The Keys Academy Trust is SAM People who can be contacted at (dpo@feps.co.uk) 01924 827869

2. Legislation and guidance

2.1 This policy meets the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and is based on guidance published by the Information Commissioner's Office (ICO) and the Department for Education. All staff and governors should note that the Act makes provision for significant fines to be levied in the event of non-compliance.

2.2 Section 5 also refers to the Education (Pupil Information) (England) Regulations 2005.

2.3 Section 6 refers to the Freedom of Information Act 2000.

3. Data protection principles and categories of data

3.1 The Data Protection Act 2018 sets out six data protection principles that the school must follow when processing personal data. Those principles are as follows:

a) Processed fairly, lawfully and in a transparent manner
b) Used for specified, explicit and legitimate purposes
c) Used in a way that is adequate, relevant and limited
d) Accurate and kept up-to-date
e) Kept no longer than is necessary
f) Processed in a manner that ensures appropriate security of the data.

3.2 The school will be responsible for, and able to demonstrate compliance with, the above data protection principles.

3.3 **Personal data:** The Data Protection Act 2018 refers to Personal data and Special categories of personal data. Personal data means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation (Article 6 lawful bases and Article 9 conditions for special category data). We will normally process personal data under the following legal grounds:

a) Where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract;
b) Where the processing is necessary to comply with a legal obligation that we are subject to, (e.g. The education act 2011);
c) Where the law otherwise allows us to process the personal data or we are carrying out a task in the public interest; and
d) Where none of the above apply then we will seek the consent of the data subject to the processing of their personal data. Schools will avoid relying on consent where there is an imbalance of power or where processing is necessary for education/public task functions.

3.3.1 **Special categories of personal data** (previously known as 'sensitive personal data') includes race, ethnic origin, politics, religion, trade union membership, biometrics, health and sexual orientation: When special category personal data is being processed, an additional legal ground must apply to that processing. We will normally only process special category personal data under following legal grounds:

a) Where the processing is necessary for employment law purposes, for example in relation to sickness absence;
b) Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
c) Where the processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and

Where none of the above apply, we will seek the consent of the data subject to the processing of their special category personal data.

Where appropriate, criminal data will be processed in line with article 10 of the UK GDPR and schedule 1 of the DPA 2018.

3.3.2 Note: the DfE consider it best practice that data such as free school meal status, pupil premium eligibility, elements of special educational need information, safeguarding information, some behaviour data and Children's Services interactions are also treated with the same care as the above special categories set out in law.

3.3.3 There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

4. Roles and responsibilities

4.1 **Data Controller**

a) Our school processes personal information relating to pupils, staff and visitors (defined as 'Data Subjects') and is therefore a Data Controller.
b) The governing body has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 2018.
c) The Headteacher will ensure the provisions of this policy are in place and that all staff are aware of their data protection obligations.
d) Day to day responsibility for Data Protection will reside with the Data Protection Officer (DPO).
e) The school is registered as a Data Controller with the ICO and renews this registration annually.

4.2 **Data Protection Lead (school-based)**

a) A Data Protection Lead within each school will be identified and will:
b) Act as the contact point for all Data Protection issues with the DPO and, with the assistance of the DPO, handle queries from Data Subjects and the ICO, e.g. for Subject Access Requests, data breaches, following the agreed procedures (see Appendix).
c) Maintain appropriate documentation related to data processing.
d) Undertake the training necessary to fulfil their role, and ensure staff have access to appropriate training and updates.
e) Monitor compliance with all aspects of Data Protection.
f) Provide advice relating to Data Protection Impact Assessments (DPIA), e.g. before introducing a new data processing system.

4.3 **School staff**

a) All school staff, in whatever role, have a duty to comply with this policy. Failure to comply may result in disciplinary action.
b) Staff must report any data related concerns or breaches immediately to the DPO.

4.4 **Data Processor**

a) The school uses a range of third parties to process data on our behalf, e.g. payroll, catering, communications. The school will ensure that all data processors are compliant with the Data Protection Act 2018.
b) In all instances, sub-processors will be subject to the terms of UK GDPR compliant written data protection agreements.

4.5 **Sharing data**

Where data is routinely shared with other organisations (e.g. Local Authority, DfE, NHS, Police), the school will ensure this is made clear in the Privacy Notice and that appropriate protocols are in place.

4.6 **The right to rectification**

If a data subject informs the Trust that personal data held about them by the Trust is inaccurate or incomplete then we will consider that request and provide a response within one month. If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the data subject within one month of their request that this is the case.

5. Data Protection documentation

5.1 **Privacy Notices**

a) The school will make available Privacy Notices for pupils/parents, staff and governors that set out how the school will make use of their personal data. These will be made available via the school website.
b) Privacy Notices will be reviewed annually or when there are significant changes to legislation or data processing activities.

5.2 **Consent**

a) Where required the school will seek and record specific consent from data subjects (e.g. image permissions, email marketing, biometrics).
b) Consent must be freely given, specific, informed and unambiguous and can be subject to withdrawal at any time.

5.3 **Data Protection Audit/record keeping/logs**

The school will maintain suitable records which detail all data that is collected, processed and where appropriate shared. In addition, the school will keep records of other key areas including the following:

a) Data Breaches – see Appendix A
b) Subject Access Requests – see Appendix B
c) Data retention schedule, disposal/destruction log
d) Data Protection Impact Assessments (DPIA)
e) Requests for changes to data
f) A general description of the technical and organisational security measures that are in place.

5.4 DPIAs are mandatory for high-risk processing activities such as biometrics, large-scale monitoring, safeguarding systems, AI implementation or new educational technologies.

5.5 **Subject Access Requests/Parental requests to see the educational record**

a) Under the Data Protection Act, pupils (or their parents for children under 13) have a right to request access to information the school holds about them. This is known as a Subject Access Request (SAR).
b) The SAR process and timescales are provided in Appendix B.
c) In addition, maintained schools, PRUs and non-maintained special schools should be aware of Regulation 5 of the Education (Pupil Information) (England) Regulations 2005 that gives parents the right of access to their child's educational record, free of charge, within 15 school days of a request.
d) The Education (Pupil Information) Regulations noted above do not apply to non-maintained schools, such as academies. Parents of children at non-maintained schools wishing to access information must therefore make a SAR.

6. Freedom of Information Act (FOI)

6.1 The school will comply with the Freedom of Information Act 2000.

6.2 All FOI requests will be directed to the DPO who will follow the procedures outlined in the Appendix C.

6.3 The school will comply with the requirement to produce a publication scheme following the guidance available from the ICO.

6.4 Where personal data is requested as part of a FOIR the request will be treated as a Data Subject Access Request and will be subject to the legislation which governs SAR provisions.

7. Security and storage

7.1 The school will ensure the following:

a) The school will ensure that appropriate technical and organisational measures are in place to protect school data.
b) The school will ensure that staff and governors are only able to access data that is relevant to their role.

7.2 The school will ensure that staff and governors are provided with specific guidance, which should include for example:

c) Use of encrypted USB flash drives/memory sticks and other removable media
d) Appropriate use of professional and personal email accounts
e) Use of encrypted/Secure email
f) Secure storage of paper files, clear desk policies, etc
g) Screen locking procedures
h) Use of cloud based storage
i) Taking data off site/Home working
j) Use of staff personal devices
k) Passwords
l) Encryption of school devices that may be taken off site, e.g. staff laptops.

Key points from the list above will be included in Staff Acceptable Use Agreements or similar.

7.3 Where data is stored on cloud-based services these should be UK based. If international data transfer is to occur, then the school should ensure appropriate safeguards are in place.

8. Retention and disposal

8.1 The school will produce a document retention and disposal schedule (see Appendix D). This will be based on the retention guidelines from the Information and Records Management Society (IRMS) Toolkit for Schools and any other guidance, e.g. DfE, Local Authority, Academy Trust, local agreements.

8.2 Appropriate measures will be taken to ensure that data that is no longer required, whether in paper or electronic form, is disposed of securely.

8.3 The school will ensure appropriate disposal of all devices that hold school data.

8.4 A destruction record will be kept for all data and devices that are disposed of.

9. Training

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

9.2 Data protection training, briefings and updates will also be provided for all staff and governors as required, but at least every two years.

10. Complaints

10.1 The school takes all concerns relating to the handling of personal data seriously and will seek to resolve any issues promptly and fairly.

10.2 Any individual who believes that the school has not complied with data protection legislation, or who wishes to raise a concern about how their personal data has been processed, should contact the school's Data Protection Officer in the first instance.

10.3 Complaints should normally be made in writing and should include sufficient detail to allow the matter to be investigated appropriately.

10.4 The school will investigate all complaints relating to data protection and will provide a response within a reasonable timescale.

10.5 Individuals also have the right to make a complaint directly to the Information Commissioner's Office (ICO) if they are dissatisfied with the school's response or believe their data has been processed unlawfully.

10.6 The ICO can be contacted at: Information Commissioner's Office: https://ico.org.uk/make-a-complaint/; Telephone: 0303 123 1113

Appendix A: Data breach information and procedures

Data protection breaches can be caused by a number of factors, e.g. Loss or theft of pupil, staff or governing body data and/or equipment or paperwork on which data is stored, inappropriate access controls allowing unauthorised use, poor data destruction procedures, human error such as sending an email to the wrong person, cyber-attack, hacking, ransomware.

In the event of a breach, the procedures below should be followed:

1. Any data protection incident should be reported immediately to the school's DPO and Headteacher.
2. If required, appropriate actions should be taken to halt the breach, and/or prevent further breaches.
3. The DPO must report any significant data protection incidents to the ICO.
    - This should take place within 72 hours of the breach being detected, where feasible.
    - If in doubt as to the significance of the incident, seek external advice, which could involve contacting the ICO.
    - If some details of the breach are yet to be determined, it would be appropriate to make an initial report to the ICO, followed up by a further report once more is known.
4. The Chair of Governors should be informed as soon as possible. Other agencies as appropriate may need to be informed depending on the breach, e.g. police, Action Fraud, social services.
5. Where the breach involves the disclosure of the personal data of specific individuals, they should usually be notified if there is a risk to their rights and freedoms.
6. The school should assess the breach risk and document the rationale for reporting/non reporting decisions
7. Fully investigate the breach, and review all related policies and procedures to make any necessary changes.
8. Provide additional training to staff as appropriate.
9. Review whether any disciplinary action should be taken.
10. If the nature of the breach could result in adverse publicity the school may wish to prepare a statement for publication.
11. A full record should be kept of all data breaches, including all the steps taken, whether reportable or not.

Additional notes

In the event of a data breach, the following areas will need to be considered:

- The type of data and its sensitivity
- What protections were in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

Appendix B: Subject Access Request (SAR) process and timescales

A SAR is a request for personal data about the applicant. Where pupils are under the age of 13, a SAR will be made on their behalf by the parent/guardian. Pupils 13 and above may make a SAR in their own right. Where a parent of a pupil 13 and above makes a SAR, it should be with the agreement of the pupil.

SARs can be made in any format, either paper or electronic, verbally in person or via telephone and should be directed to the DPO who will follow the procedure outlined below:

1. Clarify that this is a SAR and not some other request for information, i.e. a FOI request or an 'educational record' request.
2. Confirm the identity of the person making the request.
3. If it is unclear what information is being requested, ask for further details from the applicant.
4. Check that the information is available:
    - If the information is not available, inform the applicant.
    - If the information is available, note the date that the SAR was received or, in the case of further details being requested, the date that these were received. The school now has one calendar month to respond.
5. Check whether the information requested contains information about any third-party. If it does then undertake one, or more, of the following steps:
    - Seek permission to disclose the information from the third-party concerned.
    - Redact/summarise the information to protect the identity of the third-party.
    - Withhold the information to protect the rights of the third-party.
6. Ensure that the information to be supplied is clear and understandable, e.g. any complex codes or terms are explained.
7. Consider whether exemptions apply before disclosure, including safeguarding and legal/professional privilege.
8. Supply the information requested in an appropriate format, e.g. if the request is made electronically, the information should be provided in an electronic format.
9. Keep a record of the SAR and any information that was supplied.

Additional notes

- The school must provide a copy of the information free of charge. However, schools can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The school may also charge a reasonable fee to comply with requests for further copies of the same information. The fee must be based on the administrative cost of providing the information.
- The school will be able to extend the one month period of compliance by a further two months where requests are complex or numerous. If this is the case, the school must inform the applicant within one month of the receipt of the request and explain why the extension is necessary.
- The school might also decide to withhold some information. Examples of some information which (depending on the circumstances) it might be appropriate to withhold include:
    - information that might cause serious harm to the physical or mental health of the pupil or another individual;
    - information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
    - information contained in adoption and parental order records; and
    - certain information given to a court in proceedings concerning the child.
    - More information about SARs is available on the ICO website.

Appendix C: Freedom of Information (FOI) process and timescales

The school has a publication scheme, which outlines the information that is routinely made available. This can be found on the school website.

A FOI request may be made by any member of the general public, as they have a right to know about the activities of public authorities, which includes schools. The school will normally disclose the information requested in whole or part unless there is a clear and accepted reason not to do so.

All FOI requests must be in writing, either paper or electronic, and must contain the applicant's contact details. All requests should be directed to the DPO who will follow the procedure outlined below:

1. Clarify that this is a FOI request and not some other request for information, i.e. a SAR or an 'educational record' request.
2. If it is unclear what information is being requested, ask for further details from the applicant.
3. Check that the information is available:
    - If the information is not available, inform the applicant.
    - If the information is available, note the date that the FOI request was received or, in the case of further details being requested, the date that these were received. The school now has 20 school days to respond.
4. Check whether there is any good reason for refusing to disclose part or all of the information requested. Seek guidance from the ICO if in any doubt.
5. Ensure that the information to be supplied is clear and understandable.
6. Supply the information requested in an appropriate format, e.g. if the request is made electronically, the information should be provided in an electronic format.
7. Keep a record of the FOI request and any information that was supplied.

Additional notes

- The school may charge for the cost of copying and postage, where appropriate.
- The school may refuse an entire request under various circumstances, e.g.:
    - It would cost too much or take too much staff time to deal with the request (although note that the ICO guidance relating to this aspect indicates that the work required would have to be very substantial before a refusal would be acceptable).
    - Where complying might prejudice someone's commercial interests. However, it has to pass the 'Public Interest Test', i.e. that on balance the public interest in withholding the information outweighs the public interest in disclosing it.
    - The request is vexatious.
    - The request repeats a previous request from the same person.
- Further advice on when a FOI request may be refused is available from the ICO.

Appendix D: Document Retention and Disposal Schedule

https://www.gov.uk/government/publications/record-keeping-and-retention-information-for-academies/record-keeping-and-retention-information-for-academies-and-academy-trusts#how-to-dispose-of-records

	Retention Policy	Retention Period (years)	
September Destruction			
Financial records		6	
Budget management		3	
Maintenance records		6	
Lettings records		3	
Payroll		3	
Retirement records		6	
Employers Liability insurance certificate		40	
Inventory		6	
Insurance Claims		6	
Contracts under seal	date of last payment plus	12	
Contracts under signature	date of last payment plus	6	
FSM registers		6	
School meal registers		3	
Leases	expiry plus	6	
Signing in book		1	
Visitors signing in book		6	
School diaries		5	
Census		5	
Photographs		3	
Registers		7	
Pupil reports	year of leaving plus 1 year	12	cohort to be deleted
Pupil photographs	once left school	11	cohort to be deleted
SDP		3	
Admissions information		1	
Newsletters		1	
Letters to parents		1	
Pupil records			
All records passed to secondary school		n/a	
SATS results in pupil file		6	
Child protection documents in sealed envelope in pupil file	DOB plus	25	

SEND documents in sealed envelope in pupil file	DOB plus	25	
In-year transfers passed to new school		n/a	
Pupil moved abroad	DOB plus	25	
Curriculum			
Schemes, timetables, record books, mark books		1	
Pupil books	home with child at end of year	0	
Educational visit records		14	
Parental consent for trips (no major incident)	at end of trip	0	
Parental consent for trip where major incident	DOB plus	25	from year of birth - send with pupil file
Governing Body Documents			
Policies		3	
Academy status proposals		3	
Minutes and meeting documents		3	
Recruitment			
Head Teacher		6	
Unsuccessful applicants		0.5	
Personal Files	termination plus	6	
Timesheets		6	
Appraisal records		5	
H&S			
Policy		3	
Risk Assessments		3	
Incident records for injury at work		12	
Incident reports	child DOB	25	from year of birth - send with pupil file
Incident reports	adult	6	
COSHH		40	
Asbestos		40	
Fire logbooks		6	
LA/DfE			
Census		5	
Attendance returns		1	
Secondary transfer sheets		2	
Ofsted reports	life of report	life of report	
Returns to DfE		6	