The Crossley Heath School

Savile Park, Halifax, West Yorkshire HX3 0HG
Tel: 01422 360272 • Email: admin@crossleyheath.org.uk

Data Protection Policy

THE CROSSLEY HEATH SCHOOL

Version Control

Version Number	Purpose/Change	Author	Date
1	Original Policy	Jonathan Lees	07/02/2018
1.1	Approved	Governors	03/07/2018
2	Reviewed	Jonathan Lees	24/11/2020
2	Submission to B&R Governors for Approval	Paula Oldroyd	23/03/2021
3	Reviewed	Jonathan Lees	02/03/2022
4	Reviewed	Jonathan Lees	11/03/2024
5	Submission to B&R Governors for Approval	Paula Oldroyd	18/04/2024

Table of Contents

Principle elements of this policy

Purpose and Compliance	• Complies with UK GDPR and Data Protection Act 2018 to manage personal data responsibly.
Core Principles	• Lawfulness, fairness, transparency, data minimization, accuracy, storage limitation, security, accountability.
Roles and Responsibilities	• Data Controller: The school oversees data compliance. • Data Protection Officer (DPO): Monitors processes, advises staff, and ensures compliance. • Staff: Adhere to policies and report breaches.
Lawful Bases for Processing	• Includes Public Task, Legal Obligation, Vital Interests, and Consent. Consent is required for marketing, photographs, and biometric data.
Individual Rights	• Right to access, rectify, erase, or restrict data. • Right to data portability and to object to processing. • Protections against automated decision-making.
Data Management	• Privacy notices inform stakeholders. • Data securely stored with encryption and access controls. • Retention periods vary (e.g., student records retained until age 25).
Data Breach Response	• Breaches logged; significant breaches reported to the ICO. • Staff trained on reporting and managing breaches.
Data Sharing	• Shared only when legally required (e.g., with DfE, Local Authorities) and communicated transparently to parents and students.
Photographs and Biometric Data	• Consent required for marketing uses; strict rules under the Protection of Freedoms Act 2012 for biometric data.
Subject Access Requests (SARs)	• Requests addressed within one month; identity verification required; confidentiality safeguards in place.
Training and Review	• Regular staff training provided; policy reviewed biennially for compliance and relevance.

DATA PROTECTION POLICY

Next Review Date: **March 2026**
Responsibility: **Head of Compliance and IT**

STATEMENT OF INTENT

The Crossley Heath School Academy Trust Ltd is required to collect, use, and manage certain data about its staff and students in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The UK GDPR is based on the EU General Data Protection Regulation (EU) 2016/679, with changes introduced by the UK's "Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019." The Data Protection Act 2018 incorporates GDPR into UK law.

At times, the Academy may need to share personal information about staff or students with other organizations, such as the Local Authority (LA), other schools, or children's services.

This policy explains the responsibilities of staff and trustees regarding data protection and outlines how the Academy complies with the key principles of the UK GDPR.

The policy is reviewed every two years.

1. Overview of Data Protection Legislation

Data protection laws are designed to ensure that anyone collecting or managing personal data (known as "data controllers") uses it only for the stated purposes. They also ensure that individuals (known as "data subjects") are informed or can easily find out:

- What personal data is being collected about them and why.
- Whether the data is accurate and kept up to date.
- When and under what conditions the data will be shared with others.

These rules apply to both paper-based and digital records.

The principles of data protection come from the General Data Protection Regulation (GDPR). They provide guidelines for organizations to manage personal data responsibly, protect individuals' privacy, and respect their rights:

1. **Lawfulness, fairness, and transparency:** Data must be handled legally and fairly, and individuals should be clearly informed about how their data is collected, used, and shared.
2. **Purpose limitation:** Data should only be collected for specific, clear, and legitimate reasons and not used for anything outside of those purposes.
3. **Data minimization:** Only the data needed for the stated purposes should be collected.
4. **Accuracy:** Data must be accurate and, if necessary, updated. Incorrect data should be corrected or deleted promptly.
5. **Storage limitation:** Data should only be kept as long as necessary for its intended purpose.
6. **Integrity and confidentiality:** Data must be stored and processed securely to prevent unauthorized access, loss, or damage.
7. **Accountability:** Data controllers must be able to demonstrate compliance with these principles, including showing how they meet the requirements.

2. Applicable Data

In this policy, personal data refers to any information about a living person that can identify them, including things like online identifiers such as IP addresses. The GDPR applies to personal data that is:

- Stored electronically or in automated systems.
- Organized in manual filing systems based on specific criteria.
- Chronologically arranged or pseudonymized (e.g., using key codes).

The GDPR also identifies certain types of data as sensitive personal data, referred to as "special categories of personal data." This includes information about a person's genetics, biometrics, or health.

3. Data Controller

The Academy, as an organization, is the "data controller" under the law. This means it is ultimately responsible for complying with data protection regulations.

The Headteacher of the Academy is responsible for:

- Ensuring that the Academy follows the rules in the Data Protection Act, GDPR, and its own policies and procedures.
- Working with employees and their representatives to create effective data protection practices.
- Overseeing and monitoring the implementation of this policy.

4. Accountability

The Academy will take appropriate technical and organisational steps to ensure its data processing complies with the principles of the UK GDPR.

Key Measures

4.1 Transparent Privacy Policies: The Academy provides clear and detailed privacy policies to ensure transparency.

4.2 Maintaining Records for Higher-Risk Processing: Records are kept for activities involving higher-risk data, such as sensitive personal data (e.g., health or biometrics) and data related to criminal convictions.

4.3 Internal Records of Data Processing: These records include:

- The Academy's name and details.
- The purposes of data processing.
- The categories of individuals and personal data involved.
- Data retention schedules.
- Who receives the personal data.
- Security measures in place.
- Information about data transfers to other countries and safeguards for these transfers.

4.4 Data Protection by Design and Default: The Academy follows principles like:

- Collecting only the necessary data (data minimization).
- Using techniques like pseudonymization to protect data.
- Maintaining transparency about data use.
- Allowing individuals to monitor how their data is processed.
- Continuously enhancing security measures.

4.5 Data Protection Impact Assessments (DPIAs): These are conducted when needed to evaluate and manage risks in data processing.

4.6 Registration with the Information Commissioner: The Academy is registered with the Information Commissioner to ensure compliance.

5. Data Protection Officer

The Academy has a Data Protection Officer who:

- Informs and advises the Academy and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitors the Academy's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

6. Privacy Notices

The Academy has issued Privacy Notices to inform individuals about the use of their personal data. These can be found in Annex 2,3,4 and 5 or on our website.

7. Lawful Processing

There are six lawful bases for processing data under Article 6 of the GDPR.

These are as follows:

1. **Consent**: The individual has given permission for their data to be processed.
2. **Contract**: Processing is necessary to fulfil a contract the individual has entered into.
3. **Legal Obligation**: Processing is required to comply with the law.
4. **Vital Interests**: Processing is necessary to protect someone's life or wellbeing.
5. **Public Task**: Processing is needed to carry out a task in the public interest or as part of the controller's official duties.
6. **Legitimate Interest**: Processing is necessary to support legitimate interests of the controller or a third party, as long as these do not override the individual's rights or freedoms, especially for children.

7.1. Primarily, the Academy will conduct processing activities under the lawful basis of 'Public Task', exercising official authority vested in the Academy as per Article 6(1)(e) of the GDPR. This encompasses processes deemed necessary for executing tasks outlined in our 'Statement of Public Task', aligned with curriculum requirements specified in section 78 of the Education Act 2002.

7.2. Statement of Public Task: " To provide a comprehensive and well-rounded curriculum that fosters the spiritual, moral, cultural, mental, and physical development of students within the Academy and broader society, while also preparing them for the opportunities, responsibilities, and challenges they will encounter later in life. This encompasses the academy's trips, activities, and, when necessary, counselling services.".

7.3. Where the Academy processes Special Category data the legal bases used are Article 9(2)(g) of the GDPR and Schedule 1 Part 2 of the Data Protection Act 2018 in relation to statutory and government purposes, equality or opportunity of treatment and counselling.

7.4. Where a vital interest is protected the Academy will use Article 9(2)(c); and Article 9(2) (h) and (i) for the purposes of a medical diagnosis or reasons of public health.

7.5. If the Academy needs to seek consent, the Academy will obtain this under Article 6(1)(a) Consent and section 9(2)(a) Explicit Consent for Special Category Data.

7.6. The Privacy Notices provide information to the relevant data subjects as to the Academy's lawful bases for processing their personal information. Under Article 30 of the GDPR, the academy has a register of personal data it holds which details the lawful basis for processing.

8. Consent Regarding Student Data

8.1. If consent serves as the legal basis for data processing, a child aged 13 or older is considered capable of providing informed consent, provided the controller ensures the child understands the implications. Both the child and their parents may sign the consent form on Arbor if desired. For Sixth Form students, the form may be adjusted so that only the student signs it. However, in some cases, employing an alternative lawful basis might be more appropriate.

8.2. If a student or their parent/carer explicitly declines to consent to the proposed data capture or usage, the data should not be obtained or used (unless it is impractical to do otherwise, and/or the Academy has thoroughly evaluated whether refusal could potentially harm the student).

9. Biometric Data

The Academy collects and uses students' biometric data (e.g., fingerprints) and must handle this data carefully and follow the data protection legislation.

Additionally, rules from the Protection of Freedoms Act 2012 (sections 26–28) must also be followed:

Parental Notification and Consent

- Academies must inform each parent of their plan to use a child's biometric data.
- Written consent from at least one parent must be obtained before collecting or using (processing) a child's biometric data.
- This rule applies to all students under 18, and biometric data cannot be processed without written parental consent.

Restrictions on Biometric Data Processing

Biometric data cannot be processed if:

- The child objects or refuses to participate, either verbally or non-verbally.
- No parent has given written consent.
- A parent objects in writing, even if the other parent has provided consent.

Alternatives for non-participants

The Academy must offer reasonable alternative methods for students who do not participate in an automated biometric recognition system.

10. Photographs and Video

10.1. For personal use

a) The Information Commissioner, responsible for enforcing the Act, has provided guidance on photograph-taking in schools. The Act may not typically apply when photos are taken for personal use, such as among students. However, when it does apply, obtaining permission before taking photos is often sufficient to

ensure compliance. The Academy has established its own rules and procedures regarding the use of handheld devices like smartphones.

b) For the avoidance of doubt, images for personal uses (e.g. a parent photographing a child and friends at a sports day to be put in the family photo album or a grandparent filming a school play) are exempt from the Act.

10.2. For Academy use

a) Photographs taken for official academy use may be covered by the Act and students should be advised why they are being taken. In summary, it is not strictly necessary to get consent if the use is necessary for purposes connected with another lawful basis such as 'Legal Obligation' e.g. for the purposes of Identification.

b) Photographs may be captured for Marketing/Publicity purposes and used for celebrating student and staff achievements in various mediums such as press releases, the Academy website, newsletters, news articles, establishing connections with businesses, community engagement, and fundraising initiatives. Upon enrolment at the Academy, all parents provide or decline consent for their child to be featured in photographs used in school publications via the Arbor parent portal. They will receive annual reminders and can review their consent. Any parent who explicitly withholds consent for their child's photo to be used must be excluded from published photographs whenever feasible.

c) Photographs or videos of students and staff should not be utilized unless explicit consent has been obtained for their use. In the absence of explicit permission, it is improper to assume consent for the publication of such material. Prior to publication, explicit consent must be sought and obtained.

d) While most academy literature is targeted towards a specific audience, the full name of any child in a photograph should not be disclosed unless explicit consent has been obtained for such disclosure. Instead, only general labels, such as "a biology trip" should be used.

e) If pictures are being taken at an event attended by large crowds, such as a sports' day, this is regarded as a public area so the permission of everyone in the crowd shot is not needed. People in the foreground are also considered to be in a public area. However, the photographer should address those within earshot, stating where the photograph may be published and giving them the opportunity to move away. If an image of, for example, a race winner is to be used – the crowd in the background – the race winner's verbal permission should be sought and recorded using the verbal consent form. Images of students in suitable dress should only ever be used to reduce the risk of the images being disclosed inappropriately e.g. photographs of children in swimming costumes should not be used.

10.3. Photographs/Videos taken by the Press

a) Occasionally, members of the press may take photographs or film footage at the Academy e.g. at an ceremony or if the Academy is visited by a dignitary. While the press are exempt from the Act, if the Academy specifically invites the press in for a photo call, the Act applies.

b) If the Academy invites the press into school (e.g. for an awards ceremony), then the Academy needs to make students and parents/carers aware in advance that photographs at the event may appear in the press, but the Academy does not need to obtain consent in advance. Any parent/carer or child who objects to their photograph or their child's photograph appearing in the media must make this clear to the Academy.

11. Exam Results

11. 1. Examination results are classified as Personal data and not Special Category data.

11.2. The process of entering students for examinations is conducted under the lawful basis of 'Public Task', as outlined in Article 6(1)(e) of the GDPR.

11.3. The Information Commissioner has provided comprehensive guidance on the publication of exam results. The guidance recognises that such publication is likely to be necessary for the purposes of legitimate interests pursued by schools.

11.4. In rare instances, publication can result in distress. Therefore, when notifying students or their parents/carers about the publication of examination results, the academy should inform them of their right to object to publication.

12. Staff Records

12.1. Staff records are subject to the provisions of the Act. Data, including performance reviews and disciplinary warnings, is classified confidential.

12.2. Staff members who wish to review their personal file should schedule an appointment with the Executive Leader. While copies of data held in the file may be obtained, original documents must not be taken from the file. Confidential references will only be disclosed with the provider's permission.

13. Staff Health Records

13.1. Regarding sickness and ill-health records, the Academy should only keep information essential for determining an employee's fitness for work.

13.2. Information from health records should only be accessed if necessary to assess whether an employee can fulfil their managerial role, such as the Headteacher or staff appointed by the Headteacher to handle HR matters.

14. Data Collected During the Recruitment Process

14.1. Confidential references should not be disclosed unless permission is obtained from the provider. These references are exempt from the GDPR, as stated in Schedule 2, Part 4, Paragraph 24(a) of the Data Protection Act 2018, which also applies to subject access requests by the data subject.

14.2. Background checks such as Standard Disclosures and Enhanced Disclosures conducted through the Disclosure and Barring Service should not be stored in an individual's personal file. A note containing the date of the disclosure, its unique reference number, the nature of the employment for which it was requested, and any recruitment decisions made should be maintained on the individual's personal file.

14.3. When advertising for positions, the Academy will include a statement in application packs outlining the purposes for which personal information may be utilized. This statement may be concise, such as: "Personal information provided by candidates will be securely stored within the Academy and will not be disclosed to third parties external to the Academy without the individual's consent, except where legally mandated."

15. Requests for Access to Information (Subject Access Requests)

15.1. According to GDPR regulations, individuals have the right to make a subject access request, which can be communicated verbally or in written form.

15.2. If a data subject submits request electronically, it is probable that the information will be provided to the data subject in an electronic format, unless they specify otherwise.

15.3. The GDPR mandates that information must be presented in a concise, transparent, understandable, and easily accessible manner, employing clear and straightforward language. However, there is no obligation under the GDPR to translate the information for the individual.

15.4. In most instances, the Academy will not impose a fee to fulfil a subject access request. Nonetheless, if the request is deemed manifestly unfounded or excessive, the Academy reserves the right to charge a 'reasonable fee' to cover administrative costs associated with compliance. Similarly, if an individual requests additional copies of their data after an initial request, the Academy may charge a fee based on the administrative expenses of providing these additional copies.

15.5. The Academy must fulfil a subject access request within one month. If the deadline falls on a Saturday, Sunday, or bank holiday, the Academy has until the next working day to respond. Data subjects should consider the following:

- If a request is particularly complex or if the Academy has received multiple requests from the same individual, the response time can be extended by an additional two months. The individual must be informed within one month of receiving the request about the extension and the reasons for its necessity.
- While the Academy strives to fulfil requests within the month, individuals should understand that educational institutions operate differently from most organizations. There are periods, such as school holidays, trips, or activity weeks, where access to staff and data may be limited. Although the Academy aims to provide information promptly, it's possible that only part of the subject access request can be fulfilled until the school is fully staffed again. In such cases, it may be beneficial to discuss with the requester whether only a specific portion of the data record is needed, enabling a quicker response rather than waiting for a full subject access response.
- The Academy may need to request identification from an individual to verify their identity before responding to the request. It is essential for the Academy to promptly inform the individual upon receiving the request that identification is necessary. Once the Academy has received the required identification, the countdown for responding to the request commences.
- Educational Record requests as set out in The Education (Pupil Information) (England) Regulations 2005 may be treated differently to that of a SAR request.

15.6. When a child requests access to their data, the Department for Education advises exercising caution, particularly if the information could potentially upset the child. For instance, if a child expresses concern about why their school is sharing their test results with the government, the DfE suggests a more effective approach for schools would be to address the issue during lessons, incorporating a question-and-answer format alongside regular learning activities. (Source: Data Protection Toolkit for Schools, Version 1.0, August 2018, Department for Education)

15.7. In England, Wales, and Northern Ireland, unlike in Scotland, it is not automatically assumed that a child aged 12 or older possesses the necessary age and maturity to exercise their right of access. An organization must assess whether the child demonstrates sufficient maturity to comprehend their rights. Nonetheless, the right to access information about them remains with the child, rather than any other party such as a parent/carer. However, the Academy may permit a parent/carer to act on behalf of the child to exercise their rights if the child grants authorization or if it is deemed to be in the child's best interests.

15.8. If a response to a subject access request entails disclosing information that pertains not only to the requester but also to another individual, the Data Protection Act 2018 stipulates that consent from the other individual is required for disclosure, or it must be reasonable to fulfil the request without their consent.

15.9. If the Academy chooses not to fulfil the request, it must notify the individual promptly and within one month of receiving the request. The individual should be informed of the reasons for the Academy's decision, their right to lodge a complaint with the ICO or another supervisory authority, and their option to pursue legal action to enforce this right.

15.10. The Headteacher is responsible for designating individuals with the authority to disclose data requested by parents/carers and/or students, and all staff members should be knowledgeable about the procedures to follow when such requests arise. Specifically, staff should ascertain whether the requested information falls under an exempt category that is not mandated for disclosure.

16. Right to be Informed

The data subject should be informed of the reasons why the data is being held and to whom it will be disclosed. This is generally done via the Privacy Notices, and at other times when collecting or before processing personal information.

17. Right to Rectification and Erasure

17.1. The GDPR grants individuals the right to have inaccurate personal data rectified or completed if it is incomplete. The request can be made verbally or in writing. The Academy has one calendar month to respond and in certain circumstances can refuse a request for rectification.

17.2. The GDPR grants individuals the right to request the erasure of personal data under specific circumstances. However, this right is not absolute. Requests can be made verbally or in writing. The Academy must respond within one calendar month, but it may refuse a request in certain circumstances.

17.3. The data subject has the option to seek legal recourse by applying to the court for the correction or removal of inaccurate data. Ideally, measures to rectify the error would have been taken well before reaching this stage. Should a data subject file a claim, it is imperative to promptly notify the Chair of Trustees and the Headteacher.

18. Right to Restrict Processing

The GDPR provides individuals with the right to request the restriction of personal data processing under specific circumstances. However, this right is not absolute. When processing is restricted, the Academy is allowed to store the personal data but cannot utilize it. Requests can be made verbally or in writing, and the Academy must respond within one calendar month. In certain circumstances, the Academy may refuse a request. Typically, the restriction will be temporary for a specified period.

19. Right to Data Portability

According to the GDPR, individuals have the right to data portability. This right is applicable only when the lawful basis for processing is consent or for the performance of a contract, and when the processing is conducted through automated means. Since the lawful bases of consent and performance of a contract are not extensively utilized in the context of the Academy's processing, data portability may not often come into

play. However, when applicable, individuals can receive a copy of their personal data and have it transmitted from one controller to another, provided it is technically feasible and there are no legitimate reasons preventing the transmission.

20. Right to Object

The GDPR grants individuals the right to object to the processing of their personal data under specific conditions. Individuals possess an unconditional right to opt out of direct marketing, which encompasses the communication of advertising or marketing material directed at specific individuals, regardless of the means of communication.

21. Right related to Automated Decision Making and Profiling

The GDPR grants individuals specific rights concerning automated individual decision-making (decisions made solely by automated means without human involvement) and profiling (automated processing of personal data to evaluate certain aspects about an individual). In the event that the Academy intends to utilize automated decision-making or profiling, individuals will be informed accordingly.

22. Exemptions

In certain instances, both the GDPR and the Data Protection Act 2018 provide for exemptions from certain rights and obligations under specific circumstances. These exemptions are not standard procedures but are determined on a case-by-case basis.

23. Disclosure to Third Parties

All staff must understand that they are not permitted to disclose personal data to a third party without a lawful basis, as outlined in the Academy's Article 30 documentation (a comprehensive list of third parties and purposes is accessible to staff), or without the consent of the data subject. Some typical scenarios requiring specific consent include requests for an employee's home address, earnings details for mortgage purposes from a building society, or personal details of a student from a journalist. However, there may be rare instances where external entities possess a statutory right to access such information without consent.

24. Police Investigations

An exemption under the Act can be invoked if the police require information to prevent or detect crime or apprehend or prosecute a suspect. However, it's important to note that this exemption doesn't encompass all personal data in every circumstance. If the information is intended for the specified purpose and withholding it would likely hinder police efforts to prevent a crime or apprehend a suspect, then disclosure of this information is permissible.

25. Fraud Detection

Data matching for fraud detection purposes, such as verifying whether employees are receiving state benefits, is feasible. However, before the Academy engages in such a scheme, staff members will be consulted. Upon implementation, new employees must be informed of this scheme, and all employees should receive periodic reminders about it through arrangements established by the Headteacher and approved by the Trustees.

26. Pensions and Insurance Schemes

Information may be shared with a third party for purposes related to pensions and insurance schemes, provided that such sharing is deemed necessary. It is imperative that the employees involved are informed about the handling and processing of their information in this regard.

27. Required by Government or Local Authority

Both student and staff information may be periodically requested by the government or local authority. As this constitutes sensitive personal data, it is essential to limit the information shared to the minimum necessary and, whenever feasible, anonymize it.

28. Sending Data Abroad

After exiting the EU, the UK is subject to transfer regulations under its own regime. Given that this is an evolving area being continually reviewed by the UK Government, the Academy will strive to adhere to the ICO's guidance on International Transfers as it undergoes revisions.

29. Data Security and Handling Breaches

29.1. The GDPR mandates that the Academy must implement suitable technical and organizational measures proportionate with the risks, to safeguard personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage. Furthermore, the Academy must demonstrate that processing activities comply with the regulations.

The implementation of technical and organizational measures to ensure an appropriate level of security includes, among other things:

a) Pseudonymization and encryption of personal data
b) Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services
c) Ability to restore availability and access to personal data promptly in the event of a physical or technical incident
d) Regular testing, assessment, and evaluation of the effectiveness of technical and organizational measures to ensure processing security.

The Data Protection Officer will maintain a log of data breaches and potential breaches to facilitate learning from mistakes in data management. Any significant data breaches will be reported to the ICO in accordance with GDPR legislation.

29.2. The Headteacher will implement necessary measures to secure both electronic and manual files. The Academy will take appropriate steps to prevent unauthorized access to computer and manual records. Personal files must be securely stored in locked cabinets and not left exposed where unauthorized individuals may view them.

29.3. If a staff member's role at the Academy involves collecting, using, or storing personal data, the staff member has a number of legal responsibilities. These obligations apply regardless of whether the data is stored electronically or as paper records and encompass various items such as employment applications, personal details gathered for school trips, staff home telephone number lists, exam results as well as standard student and staff personal files. The staff member's responsibilities include:

a) Collecting only data that is relevant and necessary for the intended purpose;
b) Using the data solely for the specified purpose and refraining from further processing it in a manner inconsistent with those purposes;
c) Ensuring the data is accurate and up to date;
d) Safeguarding the data securely and preventing unauthorized disclosure;
e) Ensuring that the data is retained only for as long as necessary.

29.4. Employees' files, whether manual or electronic, will not be removed from the premises except in cases of emergency or with explicit authorization from the Headteacher.

29.5. The Academy's emergency plan must include provisions for securely storing backup computer data off-site. Paper records should also be securely stored, and reasonable measures should be implemented to prevent loss or damage.

30. Data Retention

30.1. A fundamental principle of the GDPR is that personal data should only be retained for as long as necessary for the purpose it was obtained. The necessity of retention will vary depending on the type of data and the assessment of associated risks, taking into account storage constraints in schools. It is unrealistic to preserve all records indefinitely, so a pragmatic approach must be adopted.

30.2. However, in case of a claim against the Academy, it's crucial to maintain appropriate records for thorough investigation and potential defence against any allegations. Students have the right to bring a claim in their own capacity once they reach the age of 18, rather than through their parents. Hence, there's a possibility of a student initiating a claim against the school up to 6 years after leaving.

30.3. Considering the above possibility, essential student records should be retained until the student reaches the age of 25. The determination of what constitutes "essential" will vary based on the individual child and any specific concerns regarding their development, welfare, or behaviour.

30.4. The table provided in Annex 3 outlines the documents that should be retained and the minimum standards for record retention. It is the responsibility of the Headteacher to establish procedures for conducting an annual review of the records held. This review aims to ensure that records are not retained longer than necessary and that expired disciplinary records are promptly removed and destroyed.

30.5. Records containing personal data should be securely destroyed through shredding or another reliable method. However, personal data processed solely for research purposes in accordance with the conditions outlined in the Act may be retained indefinitely.

31. Policy Review

The Academy will review this policy biennially and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the Academy.

Appendix A - Personal Data Sharing Guidance for staff

This guidance provides simple and clear instructions for all school staff on how to share personal data appropriately. If you're unsure about sharing information, consult a Senior Leader or the Data Protection Officer for advice.

Information Sharing Principles

When sharing personal data, always ensure it meets these key principles:

- **Lawful**: Sharing must comply with the law.
- **Necessary**: Only share what is essential.
- **Proportionate**: Share the minimum amount of information needed.
- **Need-to-know**: Only share with those who require the information.
- **Accountable**: Be able to justify your decision to share.
- **Secure**: Ensure the data is shared safely and remains protected.

Media scrutiny, particularly during sensitive incidents, highlights the importance of careful decision-making when sharing information. Always consider whether there is a valid reason to withhold information, especially in safeguarding cases. Information given in confidence usually requires consent from the individual or source before sharing.

Relevant Laws for Sharing Information

Staff must be aware of the laws that govern information sharing, especially when working with children or adults at risk:

- Common law duty of confidentiality
- UK General Data Protection Regulations (GDPR) 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- Crime and Disorder Act 1998
- Care Act 2014

The Golden Rules for Sharing Information

When sharing information with external partners, multi-agency teams, or responding to requests, follow these essential rules:

1. **Know that the law supports appropriate sharing**: The Data Protection Act and GDPR allow for responsible information sharing.
2. **Be transparent**: Clearly explain to the individual or their family why, what, how, and with whom their information will be shared.
3. **Seek advice if unsure**: If you're uncertain, consult someone appropriate while maintaining confidentiality.
4. **Respect consent**: Share information with the individual's consent whenever possible.
5. **Share without consent if necessary**: If it's in the public interest, share without consent, but base this decision on specific facts.
6. **Prioritize safety and well-being**: Ensure decisions to share information consider the potential impact on individuals and others.

7. **Follow school policies**: Adhere to rules about securely handling sensitive or confidential information, including staff records.

By following these guidelines, staff can confidently manage personal data sharing in a responsible and lawful manner.

Appendix B - Privacy Notice – Student Information

Updated: November 2024

At The Crossley Heath School Academy Trust, we take your privacy seriously. This notice explains how we collect, use, and protect student information in line with the UK GDPR and the Data Protection Act 2018.

Executive Summary

We collect and use student data to provide education, support student well-being, ensure safety, and meet legal obligations. This includes contact details, health information, academic records, and more. Data is securely stored and shared only when necessary and lawful.

What Data We Collect

We collect the following types of information about students:

- **Personal identifiers and contacts** (such as names, unique pupil numbers, contact details, and addresses)
- **Characteristics** (such as ethnicity, language, and eligibility for free school meals)
- **Safeguarding information** (such as court orders and professional involvement)
- **Special educational needs** (such as needs and rankings)
- **Medical and administrative details** (such as child health, dental health, allergies, medication, and dietary requirements)
- **Attendance records** (such as sessions attended, number of absences, reasons for absence, and previous schools attended)
- **Assessment and attainment** (such as Key Stage 2 results, post-16 course enrolment, and relevant results)
- **Behavioural information** (such as exclusions and any alternative provision in place)
- **Trips and activities** (such as dietary and medical needs, and sometimes passport numbers, birth certificates, and marriage or divorce certificates for overseas visas)
- **Catering details** (such as free school meal entitlement and purchase history)
- **ID management**: (photographs for identification badges)

Why We Collect Student Data

We collect and use student information to:

a. To help students learn better.
b. To track and share progress in learning.
c. To offer the right kind of support and care.
d. To check how well our services are doing.
e. To ensure children are safe, like noting food allergies or emergency contacts.
f. To meet our legal requirements for data collections by the Department for Education (DfE).
g. To organize and manage academy trips and activities.
h. To offer counselling services when needed.
i. To safeguard a child's important interests.

Our Legal Basis for Processing Data

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing student information are:

1. **Legal Obligation:** We process personal data because it is necessary in order to comply with the school's legal obligations and to enable it to perform tasks carried out in the public interest. We are required by The Education (Pupil Information) (England) Regulations 2005 to maintain a Pupil's Educational Record.

2. **Public Task:** To perform tasks in the public interest, such as delivering education.

3. **Vital Interests:** To protect students in emergencies.

4. **Consent:** For specific purposes where required, such as using photos for promotional materials.

How We Store and Protect Data

Student data is securely stored following our data retention policies. We use encryption, access controls, and regular audits to protect all information.

Who We Share Data With

For us to legally, effectively and efficiently function we are required to share data with appropriate third parties, including but not limited to:

- **Local Authority**: To fulfil legal obligations, including sharing information on safeguarding concerns and exclusions.
- **Department for Education**: To comply with legal requirements for data sharing.
- **Pupil's Family and Representatives**: For emergency situations and related communications.
- **Educators and Examining Bodies**: To ensure compliance with examination regulations and maintain the integrity of assessments.
- **Ofsted**: As part of school inspections and reporting processes.
- **Suppliers and Service Providers**: To deliver contracted services effectively.
- **Central and Local Government**: To support governance and policy implementation.
- **Auditors**: To verify compliance with legal and financial obligations.
- **Health Authorities (NHS):** To promote and safeguard pupil wellbeing.
- **Health and Social Welfare Organisations**: To support the health and welfare of pupils.
- **Youth Support Services**: To enable C&K careers to provide post-16 education and careers advice.
- **Professional Advisers and Consultants**: To enhance service delivery and uphold our public service standards.
- **Charities and Voluntary Organisations**: For collaborative and supportive initiatives.
- **Police, Courts, Tribunals, and Security Services**: To ensure safety and security within the school community.
- **Professional Bodies**: For compliance and development in education practices.
- **Receiving Schools**: To facilitate smooth transitions for pupils after they leave.

For further information about who we share data with and why please see Appendix A (on website).

Department for Information (DfE) National Pupil Database

We are required to provide information about you to the DfE as part of data collections such as the school census. Some of this information is then stored in the National Pupil Database, which is managed by the DfE and provides evidence on how schools are performing. The database is held so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others. The DfE may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the DfE's webpage on how it collects and shares research data. You can also contact the Department for Education if you have any questions about the database.

Your Data Rights

Under data protection laws, you have the right to:

- Access your or your child's data
- Request corrections to inaccurate information
- Object to data processing in certain circumstances
- Request deletion of data where applicable
- Raise concerns with the Information Commissioner's Office (ICO)

Contact Us

For questions about this notice or to exercise your rights, please contact our Data Protection Officer:
Mr. Jonathan Lees
Email: dpo@crossleyheath.org.uk
Telephone: 01422 360272

Appendix C

The Crossley Heath School Academy Trust
Privacy Notice – Workforce Information

At The Crossley Heath School Academy Trust, we oversee the management of workforce information in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This document is designed to outline our approach to handling student data under our care.

The UK GDPR, which originated from the EU in 2018, has been adapted for the UK following its exit from the EU in 2019. Put simply, whenever we refer to GDPR in this document or related Academy materials, we're talking about the UK-specific version.

The categories of workforce information that we process include:

- **Personal information** (such as name, employee or teacher number, national insurance number)
- **Characteristics information** (such as gender, age, ethnic group)
- **Contract information** (such as start date, hours worked, post, roles and salary information)
- **Work absence information** (such as number of absences and reasons)
- Q**ualifications** (and, where relevant, subjects taught)
- **Result of Disclosure and Barring Service** (DBS) check
- **Contact information** (such as address, telephone number, email address, emergency contact details)
- **Pecuniary interests outside of academy** (which are deemed a conflict of interest)
- **Medical information** (such as medical needs, doctors information, GP statement of fitness to work.)
- **Payroll** (such as bank details, salary scale, wage, deduction of earnings, pension, tax and National Insurance)
- **Trips and activities** (dietary needs, medical needs and history and in some cases for overseas trips - passport numbers, birth certificates and divorce and marriage certificates for visas)
- I**D Management** (photographs and names for identification badges)
- **Proof of right to work in the UK**
- **CCTV Images**

This is not an exhaustive list. For the current categories of information we process, please contact Mr Jonathan Lees (DPO) at the school.

Why we collect and use workforce information

We collect and use workforce information, for the following purposes:

a) enable the development of a comprehensive picture of the workforce and how it is deployed
b) inform the development of recruitment and retention policies
c) enable individuals to be paid
d) to keep children safe
e) to meet the statutory duties placed upon us.
f) to facilitate school trips and activities
g) to protect the vital interests of an employee

Under the General Data Protection Regulation (GDPR), the legal basis / bases we rely on for processing personal information for general purposes are:

Legal Obligation: Article 6(1)(c) of the GDPR for any statutory *processing which is necessary for compliance with a legal obligation to which we are subjected. This relates to tasks (c) (d) and (e) and includes the following statutory guidance:*

- Section 537A of the Education Act 1996, 17
- The Education Act 1996 S29(3)
- The Education (School Performance Information) (England) Regulations 2007
- *regulations 5 and 8 School Information (England) Regulations 2008*
- the Education (Pupil Registration) (England) (Amendment) Regulations 2013
- Education and Skills Act 2008
- DfE Keeping Children Safe in Education Guidance 2016
- *DfE Working Together to Safeguard Children (2015)*
- the Management of Health & Safety at Work Regulations 1999,
- Regulatory Reform (Fire Safety) Order 2005 England and Wales.
- Health and Safety at Work Act 1974
- the Disability Discrimination Act 1995
- Immigration, Asylum and Nationality Act 2006
- Employment Rights Act 1996
- Employment Relations Act 2004
- The Race Relations Act, 1976
- Employment Rights Act 1996 (Itemised Pay Statement) (Amendment) Order 2018

We may process workforce personal data in accordance with a 'Public Task': Public interest or in the exercise of an official authority vested in us Article 6(1)(e) of the GDPR. This relates to task (f) and includes any process which is for necessary for the exercise of a task we have termed our 'Statement of Public Task', which is based on the curriculum requirements of section 78 of the Education Act 2002:

Statement of Public Task: *"To deliver a balanced and broadly based curriculum which - promotes the spiritual, moral, cultural, mental and physical development of students at the academy and society, and prepares pupils for the opportunities, responsibilities and experiences of later life. This includes academy trips and activities; and where appropriate counselling services".*

Vital Interests: Article 6(1)(d) of the GDPR. Where the vital interests of an individual are at risk we will use Vital Interests as a lawful basis. This relates to task (g). If we need to seek consent, we will obtain this under Article 6(1)(a) Consent and section 9(2)(a)

Explicit Consent for Special Category Data: In addition, concerning any special category data we use Article 9(2)(g) of the GDPR and Schedule 1 Part 2 of the Data Protection Act 2018 in relation to statutory and government purposes, equality or opportunity of treatment and counselling. Where a vital interest is protected, we will use Article 9(2)(c); and Article 9(2) (h) and (i) for the purposes of a medical diagnosis or reasons of public health.

Collecting workforce information

We collect personal information via paper-based or electronic forms via the Executive Leader or the Arbor system.

Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis.
In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing personal data
The school will create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment has ended, the school will retain this file and delete the information in accordance with our data retention policy.
Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, the school will shred or incinerate paper-based records and override electronic files. The school may also use an outside company to safely dispose of electronic records.

Who we share the information with:

We routinely share this information with:

- Our local Authority
- The Department for Education (DfE)
- Payroll and HR Services
- The School's Absence and Insurance Provider

Why the school may share workforce information

The school does not share personal data with any third party without your consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law) the school may share personal data with:

- the Department for Education (DfE) on a statutory basis. This data sharing underpins
- workforce policy monitoring, evaluation, and links to school funding / expenditure and the
- assessment educational attainment.
- the local authority – to meet our legal obligations to share certain information with it, such as
- safeguarding concerns and information about Headteacher performance and staff dismissals
- The school also uses various systems, such as assessment and reporting software, communication
- systems and curriculum software that may process personal data. As the data controller the school
- will ensure that processors meet and uphold the required data protection standards. An up-to-date
- list of these third parties can be found on the school website.
- How Government uses your data?
- The workforce data that we lawfully share with the DfE through data collections:
- informs departmental policy on pay and the monitoring of the effectiveness and
- diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

• conducting research or analysis
• producing statistics
• providing information, advice or guidance

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

• who is requesting the data
• the purpose for which it is required

• the level and sensitivity of data requested; and
• the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

To contact the department: https://www.gov.uk/contact-dfe

Your rights

How to access personal information the school holds about you:

Individuals have a right to make a 'subject access request' to gain access to personal information held. If you make a subject access request, and if the school does hold information about you, the school will:

- give you a description of it
- tell you why the school is holding and processing it, and how long it will be kept for
- explain where the school got it from, if not from you
- tell you who it has been, or will be, shared with
- let you know whether any automated decision-making is being applied to the data, and any
- consequences of this
- give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances. If you would like to make a subject access request, please contact the DPO (Jonathan Lees)

Other rights regarding personal data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- object to the use of your personal data if it would cause, or is causing, damage or distress
- object to the use of your personal data for decisions being taken by automated means (by a
- computer or machine, rather than by a person)
- in certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or
- restrict processing
- claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact the DPO.

Complaints

We take any complaints about the collection and use of personal information very seriously. If you think that the collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about data processing, please raise this with the school in the first instance.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113

Appendix D

The Crossley Heath School Academy Trust
Privacy Notice – Ex-Alumni and Friends

At The Crossley Heath School Academy Trust, we oversee the management of workforce information in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This document is designed to outline our approach to handling student data under our care.

The UK GDPR, which originated from the EU in 2018, has been adapted for the UK following its exit from the EU in 2019. Put simply, whenever we refer to GDPR in this document or related Academy materials, we're talking about the UK-specific version.

What information the school will process and why
The school and any relevant other organisation will use the contact details of alumni and other members of the school community to keep them updated about the activities of the school, or alumni events of interest, including by sending updates and newsletters, by email and by post.

Information which may be processed includes:

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- career information
- bank details and other financial information, e.g. where events are paid for or
- donations made;
- correspondence with and concerning staff, pupils and parents past and present;
- images from alumni events, and images captured by the school's CCTV system; and
- where appropriate, information about individuals' health and welfare, and contact
- details for their next of kin.

The use of personal data will be made in accordance with the school's legitimate interests, provided that these are not outweighed by the impact on individuals and provided it does not involve special or sensitive types of data.

The school expects that the following uses will also fall within that category of its "Legitimate interests":

- Maintaining a record of those who were educated at The Crossley Heath School Academy
- Trust Limited.
- Maintaining relationships with alumni and the school community, including direct
- marketing or fundraising activity;
- For the purposes of donor due diligence, and to confirm the identity of prospective
- donors and their background and relevant interests; including collecting information
- from publicly available sources about occupation and activities, in order to maximise
- the school's fundraising potential.
- To make use of photographic images in school publications, on the school website
- and (where appropriate) on the school's social media channels;
- To give and receive information and references about past pupils, including to any
- educational institution that it is proposed they attend; and to provide references to
- potential employers;
- To carry out or cooperate with any school or external complaints, disciplinary or

Unless the relevant individual objects, the school will also:

- Share personal data about alumni, as appropriate, with organisations set up to help
- establish and maintain relationships with the school community;
- Contact alumni by post, email and phone in order to promote and raise funds for
- the school and, where appropriate, other worthy causes;

Should you wish to limit or object to any such use, or would like further information about how the school uses your personal information, please contact the school by email at dpo@crossleyheath.org.uk; or by post to the school address. You always have the right to object to direct marketing or fundraising. However, the school is nonetheless likely to retain some of your details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

How the school collects and processes your data

Generally, the school receives personal data from the individual directly. This may be via a form, or simply in the ordinary course of interaction or communication such as email. To ensure that the school's communications are relevant to you and your interests and to assess your likely ability to make, and interest in making, donations to the school, it may use additional information such as geographical information and measures of affluence where available from external sources to assist.

The school wants to make sure it uses it's resources as effectively as possible to help the school engage with its community of alumni and friends appropriately. In order to achieve this the school may undertake wealth screening of the alumni database. Wealth screening enables the school to better target conversations about fundraising and therefore generate funds cost- effectively. To achieve this the school may share your data with trusted third-party suppliers.

In order to provide you with the best experience and understand how the school could engage with you in the future, it undertakes analysis on the personal data it holds on you. This analysis helps the school to gain a better understanding of your interests, of how you engage with the school, and to understand broader demographic and geographic trends.

The school may also undertake research on your personal information to help make informed decisions. This may include research on demographic, philanthropic, business and financial information from publicly available sources, including social media. The school may also combine the data you provide with data obtained from other sources.
If you do not wish your data to be used in any of the ways listed above or have questions about this, you can contact the school.

Who has access to personal data and who the school shares it with

For the most part, personal data collected by the school will remain within the school, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis).

Some of the school's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the school's specific directions.

How long the school keeps personal data

The school will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Alumni information is kept for the duration of the relationship between the alumni and the school.

Requesting access to your personal data

According to data protection laws, parents and students have the right to ask for access to the information we hold about them. If you'd like to request your personal information or access your child's educational record, please contact:

The Data Protection Officer:
Mr Jonathan Lees
The Crossley Heath School
Savile Park
Halifax
HX3 0HG
dpo@crossleyheath.org.uk
Telephone: 01422 360272

You also have the right to:

- Object to the processing of personal data if it's likely to cause damage or distress.
- Stop your data from being used for direct marketing.
- Object to decisions made by automated processes.
- Request corrections to inaccurate personal data, or have it blocked, erased, or destroyed under certain circumstances.
- Seek resolution either through the ICO or the courts if needed.

If you're worried or unhappy about how we're collecting or using your personal data, please talk to us first. You can also contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Consent

Where the school is relying on consent as a means to process personal data, any person may withdraw this consent at any time. Please be aware however that the school may have another lawful reason to process the personal data in question.

Data accuracy and security

The school 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 please notify the DPO of any significant changes to important
information such as contact details held about them.

An individual has the right to request that any out-of-date, irrelevant or inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under data protection law): please see above for details of why the school may need to process your data, or who you may contact if you disagree.
The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to school systems. All staff and governors will be made aware of this policy and their duties under data protection law and receive relevant training.

Queries and Complaints

We take any complaints about the collection and use of personal information very seriously. If you

think that the collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about data processing, please raise this with the school in the first instance.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113

Appendix E

Record retention schedule

Type of Data	Recommended period for retention
Students	
Admission documents relating to the Admissions test	**Unsuccessful candidates:** 1 year. **Withdrawals:** 1 year. **Successful candidates:** 1 year after admission
Exam Scripts – External (Including Admissions Test)	The exam boards hold onto papers as per their regulations. Nevertheless, if a student lodges an appeal with the exam board regarding their final grade, they might also file a claim against the Academy for inadequate education. Retain any pertinent student data if complaints or concerns arise during the student's course.
Exam Scripts – Internal	These documents offer valuable insight into a student's abilities and pinpoint areas of difficulty. The Academy can return exam papers or offer copies to students for review after the exam but reserves the right to retain the original papers. A record of marks should be maintained in a student's file until they reach the age of 25.
Pupil Educational Record	Student's DOB + 25 years
Coursework	Once coursework is no longer required, the Academy has the option to give it back to the student, store it, or dispose of it, as long as any exam board appeal period has elapsed. If students take exams with multiple exam boards, it might be easier administratively to establish a deadline for keeping coursework based on the final appeal date. A selection of coursework showcasing the Year Group's diversity, along with records of the marks received, may be kept for reference.
Photographs	Photographs serve various purposes in schools, including identification, educational, and marketing. Each use should be treated separately and may have different conditions for processing. Photos collected and utilized based on one lawful basis shouldn't be repurposed for a different lawful basis, especially after a student has left. For instance, if a photo was initially taken for educational purposes as part of the Academy's Public Task, it shouldn't be later used for marketing without reassessing its legality. Upon a student's departure, the Academy must evaluate whether the photo still fits the lawful basis for its collection to avoid unauthorized processing. If a photo was used for marketing while the individual was a student, consent must be obtained to continue using it for marketing afterward. Additionally, photos shouldn't be retained longer than necessary for their intended purpose.
Registers	6 years from the date the data was entered (DfE guidance - Working together to improve school attendance paragraph 36)
School Trips – Risk Assessments and General Paperwork	Keep records for one year for future planning purposes unless any issues arise. In such cases, retain the records until the relevant student(s) reach the age of 25.
School Trips – Permission Slips	Typically, keep records for one month after a trip if there are no issues. However, if any problems occur, hold onto the records until the relevant student(s) reach the age of 25.

Type of Data	Recommended period for retention
Staff	

Staff records	In general, retain records for six years after the end of employment. Please refer below for specific document retention periods. Note: Disciplinary records should be deleted according to the time limits outlined in the disciplinary procedures.
Written particulars of employment, contracts of employments and changes to terms and conditions	6 years from end of employment.
Application form (and other recruitment materials including notes of phone calls made/received)	6 months from end of employment (or six months from date of rejection).
Applications for jobs – where the candidate is unsuccessful	6 months (recommended by The Discrimination Acts 1975 and 1986 and the Race Relations Act 1976).
References received	1 year from date received unless person employed in which case 6 years from end of employment.
References given/information to enable reference to be provided	6 years from reference/end of employment.
Induction and training records	6 years from end of employment.
Records related to promotion, transfer, training and disciplinary matters	6 years from end of employment. Disciplinary matters, depending on the issue but not more than 6 years from end of employment.
Summary of record of services e.g. Name, position held, dates of employment	6 years from end of employment.
References provided for ex-employees	5 years.
Police Checks – DBS Disclosures	Date of disclosure and unique reference number 6 years from end of employment.
Expense accounts	6 years
Sickness records	3 years after the end of each tax year for Statutory Sickness Pay purposes.
Maternity records	3 years from the end of the tax year in which maternity pay period ends.
Annual leave records	2 years from the end of annual leave year, or longer if leave carried over
Unpaid leave / Special leave records	6 years from the date on which made.
Annual appraisal / assessment records	6 years from end of employment.
Photographs	Photographs serve various purposes in schools, including identification, educational, and marketing. Each use should be treated separately and may have different conditions for processing. Photos collected and utilized based on one lawful basis shouldn't be repurposed for a different lawful basis, especially after a member of staff has left. For instance, if a photo was initially taken for educational purposes as part of the Academy's Public Task, it shouldn't be later used for marketing

	without reassessing its legality. Upon a member of staff's departure, the Academy must evaluate whether the photo still fits the lawful basis for its collection to avoid unauthorized processing. If a photo was used for marketing while the individual was a student, consent must be obtained to continue using it for marketing afterward. Additionally, photos shouldn't be retained longer than necessary for their intended purpose.
Health and Safety records	3 years (personal injury time limit).
Pension records related to employees	12 years after benefit ceases.
Summary staff record (i.e. period of employment and other basic information, including details of unpaid absences, pension related information, and records relating to an accident or injury at work).	Until individual is aged 72