KING EDWARD VI FOUNDATION BIRMINGHAM

Educational excellence for our City

KING EDWARD VI ACADEMY TRUST BIRMINGHAM

Data Protection Policy & Data Processing Procedures

Responsible Board/Committee	Academy Trust Board Foundation Board
Policy Type	Central Policy (Group A)
Policy Owner	Risk and Compliance
Statutory	Yes
Publish Online	Yes
Last Review Date	June 2026
Review Cycle	Annual This policy will not expire but will be reviewed as per its designated cycle. This policy remains effective whilst the review is taking place and will only become non-applicable once the updated version has been approved.
Next Review Date	June 2027
Version	3

Contents

Purpose 3

Definitions 3

Roles and Responsibilities 4

Procedures 4

Adherence to the UK GDPR 4

Conditions for Processing 5

Use of Personal Data by the Foundation and Academy Trust 5

Pupils 5

Staff 6

Third Parties 7

Disclosure of Personal Data to Third Parties 7

Other Rights of Individuals 8

Right to Object to Processing 8

Right to Withdraw Consent 8

Right to be Informed 8

Right to Data Portability 8

Right to Rectification 8

Right to Erasure 9

Right to Restrict Processing 9

Right of access 10

References, Legislation, and Guidance 10

Appendix A: Data Processing Checklist 11

Appendix B: Processing Special Categories and Criminal Convictions Data 13

Appendix C: Data Breach Process 15

Appendix D: Subject Access Requests 16

Appendix E: Freedom of Information Requests 18

Appendix F: Data Retention Schedule 20

Purpose

The Schools of King Edward VI in Birmingham (the "Foundation") and the King Edward VI Academy Trust Birmingham (the "Academy Trust") collect and use certain types of personal information about staff, pupils, parents, and other individuals who come into contact with the Foundation and Academy Trust in order to provide education and associated functions. Both entities are required by law to collect and use certain types of information to comply with statutory obligations related to employment, education, and safeguarding. This policy is intended to ensure that personal information is dealt with properly, securely, and in accordance with the law. For the purposes of cooperation between the two legal entities, data collected in accordance with this policy may be shared between the Foundation and Academy Trust. In these scenarios, both entities act as data controller and processor.

The UK GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one in which the data is structured in such a way that it is searchable based on specific criteria (for example, you would be able to use something like the individual's name to find their information). If this is the case, it does not matter whether the information is in a different physical location.

The appendices to this policy detail how data is processed, including the processing of special category and criminal conviction data. Additionally, the process for handling data/information requests, retention periods, and the data breach process.

Definitions

'Personal data' is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain.

A subset of personal data is known as 'special category personal data'. This special category data is information that reveals:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health
- An individual's sex life or sexual orientation

- Genetic or biometric data for the purpose of uniquely identifying a natural person

Special category data is given enhanced protection, and additional safeguards apply - please see Appendix B for more details. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

The Foundation and Academy Trust do not intend to seek or hold special category data (previously known as sensitive personal data) about staff or students except where the Foundation or Academy Trust has been notified of the information, or it comes to the Foundation or Academy Trust's attention via legitimate means (e.g., a grievance), or it needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to the Foundation or Academy Trust their race or ethnic origin, political or religious beliefs, whether they are a trade union member, or details of their sexual life (save to the extent that details of marital status and/or parenthood are needed for other purposes, e.g., pension entitlements).

Roles and Responsibilities

Data Protection Officer (DPO)
The DPO is an independent expert who assists us in monitoring internal compliance, informs and advises us on data protection obligations and data protection impact assessments, and acts as a contact point with the Information Commissioner's Office. The DPO is GDPR Sentry.

Data Protection Leads (DPL)
Each school has a DPL who acts as a champion for good data protection practices in their school.

All employees
All employees will likely have a role in handling, using, or managing the personal data that the Foundation and Academy Trust control. All employees are, therefore, required to act in accordance with the data protection policies, procedures, and associated appendices, as well as the relevant legislation. This means that the DPLs are not solely responsible for data protection - all employees are responsible for this.

Procedures

Adherence to the UK GDPR

The Foundation and Academy Trust will adhere to the data protection principles as outlined in the UK GDPR:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/

The Foundation and Academy Trust are committed to complying with these principles. They will:

- Inform individuals about how and why we process their personal data through privacy notices.

- Be responsible for checking the quality and accuracy of the information.
- Regularly review the records held to ensure that information is not held longer than is necessary and that it has been held in accordance with the data retention period (see Appendix F).
- Ensure that when information is authorised for disposal, it is done appropriately.
- Ensure appropriate security measures to safeguard personal information, whether it is held in paper files or on our computer system, and always follow the relevant security policy requirements.
- Share personal information with others only when it is necessary and legally appropriate to do so.
- Set out clear procedures for responding to requests for access to personal information, known as subject access requests.
- Report any breaches of the GDPR in accordance with the procedure outlined in Appendix C.

Conditions for Processing

The conditions under which we will process personal data are as follows:

- The individual has given consent that is specific to the processing activity, and that consent is informed, unambiguous, and freely given.
- The processing is necessary for the performance of a contract to which the individual is a party or is necessary for the purpose of taking steps regarding entering a contract with the individual at their request.
- The processing is necessary for the performance of a legal obligation to which we are subject.
- The processing is necessary to protect the vital interests of the individual or another.
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us.
- Where we have a legitimate interest.

Use of Personal Data by the Foundation and Academy Trust

The Foundation and Academy Trust processes personal data on pupils, staff, trainee teachers, governors/trustees, and other individuals such as visitors. In each case, the personal data must be processed in accordance with the data protection principles.

In addition to traditional data processing activities, we also engage in processing personal data through Artificial Intelligence (AI) systems. These systems, used for purposes such as enhancing educational experiences and operational efficiency, are also covered under this policy. We ensure that AI systems processing personal data are designed and operated transparently, uphold fairness, and are subject to ongoing scrutiny to prevent biases and protect the rights of individuals. In the context of AI, we ensure that we also comply with our AI principles as well as data protection principles.

Pupils

- The personal data held regarding pupils includes contact details, assessment/examination results, attendance information, characteristics such as ethnic group (if provided), special educational needs, any relevant medical information, biometric information, CCTV images, electronic sign-in data, and photographs.
- The data is used to support the education of the pupils, monitor and report on their progress, provide appropriate pastoral care, and assess how well the school/academy is doing, together with any other uses normally associated with this provision in a school environment.
- The Foundation and Academy Trust may make use of limited personal data (such as contact details) relating to pupils and their parents or guardians for fundraising, marketing, or promotional purposes and to maintain relationships with their pupils, but only where consent has been provided for this. They may:

    - Transfer information to any association, society, or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing, or promotional purposes relating to the Academy, but only where consent has been obtained first.
    - Make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities.
    - Keep the pupil's previous school informed of their academic progress and achievements.
    - Use photographs of pupils in accordance with the photograph policy.

Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardians, the Foundation and Academy Trust will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the Academy Trust believes disclosure will be in the best interests of the pupil or other pupils. Disclosure for safeguarding purposes will be lawful because it will be in the substantial public interest.

Staff

- The personal data held about staff will include contact details, employment history, information relating to career progression and job performance, information relating to DBS and other checks, occupational pensions, CCTV images, electronic sign-in data, and photographs.
- The data is used to comply with legal obligations in relation to employment and the education of children in a school environment. The Foundation/Academy Trust may pass information to other regulatory authorities where appropriate and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.
- Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.
- DBS and other checks are carried out based on the legal obligations in relation to the safer recruitment of Staff as stipulated in the Education (Independent School Standards) Regulations, and the DBS information (which will include personal data relating to

criminal convictions and offences) is further processed in the substantial public interest, with the objective of safeguarding children.

- Access to the DBS information is restricted to staff who have a genuine need to have access to it for their job roles. In addition to the provisions of the GDPR and the Data Protection Act 2018, disclosure of this information is restricted by Section 124 of the Police Act 1997, and disclosure to third parties will only be made if it is determined to be lawful.

Third Parties

- The Foundation and Academy Trust may hold personal information in relation to other individuals who have contact with them, such as volunteers and guests. Such information shall be held only in accordance with data protection principles and shall not be kept longer than necessary. This may include CCTV images and electronic sign-in data.
- Any wish to limit or object to the uses to which personal data is put should be notified to the Data Protection Officer, who will ensure that this is recorded and adhered to if appropriate. If the Data Protection Officer is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the Foundation and/or Academy Trust cannot comply with their request.

Disclosure of Personal Data to Third Parties

The following list includes the most common reasons that the Foundation and Academy Trust will authorise disclosure of personal data to a third party:

- To give a confidential reference relating to a current or former employee, volunteer, or pupil.
- For the prevention or detection of crime.
- For the assessment of any tax or duty.
- Where it is necessary to exercise a right or obligation conferred or imposed by law.
- For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings).
- For the purpose of obtaining legal advice.
- For research, historical, and statistical purposes (so long as this neither supports decisions in relation to individuals nor causes substantial damage or distress).
- To publish the results of public examinations or other achievements of pupils.
- To disclose details of a pupil's medical condition where it is in the pupil's interests to do so and there is a legal basis for doing so. For example, for medical advice, insurance purposes, or to organisers of school trips. The legal basis will vary in each case but will usually be based on explicit consent, the vital interests of the child, or reasons of substantial public or legitimate interest (usually safeguarding the child or other individuals).
- To provide information to another educational establishment to which a pupil is transferring.
- To provide information to the Examination Authority as part of the examination process.
- To provide information to the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

Please see Appendices D and E for details regarding data and information requests.

Other Rights of Individuals

Right to Object to Processing

An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest where they do not believe that those grounds are adequately established.

Where such an objection is made, the recipient must send it to the Data Protection Officer within two working days of receipt. The Data Protection Officer will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights, and freedoms of the individuals or whether the information is required to establish, exercise, or defend legal proceedings.

The Data Protection Officer shall be responsible for notifying the individual of the outcome of their assessment within 15 working days of receipt of the objection.

Right to Withdraw Consent

If individuals have consented to their personal data being processed, they may withdraw this consent at any time.

Right to be Informed

Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection, and where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

- If the personal data is used to communicate with the data subject, when the first communication is made; or
- if the personal data is to be transferred to another party before that transfer is made; or
- as soon as reasonably possible and, in any event, not later than one month after the personal data is obtained.

Right to Data Portability

Individuals have the right to request that data provided to the Academy Trust/Foundation be transmitted directly to another controller. This right only applies when:

- The lawful basis for processing this information is consent **or** for the performance of a contract; and
- the processing is carried out by automated means.

Right to Rectification

An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent by the recipient to the Data Protection Officer within two working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable and the individual notified.

Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual. The individual shall be given the option of directly appealing to the Information Commissioner.

An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to Erasure

Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed.
- Where consent is withdrawn, and there is no other legal basis for the processing, or where an objection has been raised under the right to object and found to be legitimate.
- Where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met).
- Where there is a legal obligation on the Foundation and/or Academy Trust to delete.
- The Data Protection Officer will decide any application for erasure of personal data and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers and/or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to Restrict Processing

In the following circumstances, the processing of an individual's personal data may be restricted:

- Where the accuracy of data has been contested during the period when the Foundation and/or Academy Trust is attempting to verify the accuracy of the data.
- Where processing has been found to be unlawful and the individual has asked that there be a restriction on processing rather than erasure.
- Where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise, or defence of a legal claim.
- Where there has been an objection made under the right to erasure, pending the outcome of any decision.

If an individual wants to send their personal data to another organisation, they have a right to request that the Foundation and/or Academy Trust provide their information in a structured,

commonly used, and machine-readable format. As this right is limited to situations where the Academy Trust is processing the information based on consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If this request is made, it should be forwarded to the Data Protection Officer within two working days of receipt, and the Data Protection Officer will review and revert as necessary.

Right of access

An individual has the right of access to personal data held about them. Please see Appendix D, which outlines the process relating to this right.

Compliance and monitoring

The Foundation and Academy Trust will take reasonable steps to ensure that staff members will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR. The Foundation and Academy Trust will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

Please refer to the IT policies for further details.

References, Legislation, and Guidance

This policy is based on the UK GDPR. More information can be found here: https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/. The ICO is the supervisory authority under UK GDPR, and data subjects have the right to complain to the ICO.

If you have any questions regarding this policy, please contact: riskandcompliance@kevibham.org.

If you need to contact our Data Protection Officer, please contact: support@gdprsentry.com

Related policies:

- IT Policies
- Privacy Notices

Appendix A: Data Processing Checklist

A.1 This checklist should be used whenever you are using a third party to deal with personal data on your behalf. You will continue to be responsible for the information, and the third party will be restricted to doing only what you tell them. They will have no right to keep or use the information for any of their own purposes. You will be the Data Controller, and the third party is the Data Processor.

A.2 Controllers are required to use only processors that provide sufficient guarantees to implement appropriate data protection measures and ensure compliance. Adherence of a processor to an approved code of conduct or approved certification assists in demonstrating that sufficient guarantees exist. We recommend that the Processor's adherence to an approved code of conduct or certification should be specified in your agreement with the Processor.

A.3 To comply with the law, your agreement with the Processor must be in writing and contain the following:

- Its subject matter and duration.
- The nature and purpose of the processing.
- The type of personal data.
- The categories of individuals who are the data subjects.
- Expressly state that the Processor can only act on your instructions as the Controller.
- Require the Processor to impose a duty of confidentiality on relevant staff.
- Require the Processor to implement relevant security measures to protect the data. You can specify what those measures are, and what you impose will depend upon the type and sensitivity of the information.
- Require the Processor to seek your prior written permission as Controller to engage a sub-contractor.
- Require the Processor to make all necessary arrangements to ensure that, as the Controller, you can respect the rights of the individuals under data protection law. As an example, the Processor must be required to make available any personal data should an individual make a Subject Access Request. They must be able to delete or rectify data if necessary and must enable data portability where applicable.
- Require the Data Processor to have in place the necessary means of assisting you as the Controller to meet your obligations under data protection law. This includes ensuring the security of data, cooperating in relation to your notification of breaches to the Information Commissioner's Office and data subjects, and preparing data protection impact assessments.
- Require the Processor to assist you as the Controller in meeting any obligations imposed by the Information Commissioner's Office by allowing access to information and details of activities and systems when required.
- Require the Processor to delete or return the data at the end of the contract. Whether the data is returned or deleted is your decision as the Controller.

- Require the Processor to provide you with all necessary information regarding processing activities to demonstrate compliance, including security measures taken, disclosures made, what has been done to the information, plus anything else you need to know as Controller to allow the processing to be audited.
- Provide that any legal requirements that the Processor is subject to which may require the disclosure of the personal data (such as Freedom of Information) should be notified to you as the Controller in advance, where possible.
- Be governed by the law of England and Wales or an EU member state.

Note: The GDPR refers to the possible development of standard clauses covering the compliance matters listed above. The position should, therefore, be monitored.

CHECKLIST

☐ Agreement is in writing under the law of England and Wales or the law of the EU or other member state

☐ Names and details of the processer and controller

☐ Details of the processing project, its purpose, subject matter, and duration

☐ The Processor can only act on the instructions of the Controller

☐ Duty of confidentiality for the Processor's staff

☐ Processor to implement the necessary security measures

☐ Only sub-contract with the Controller's permission

☐ Make arrangements which allow the Controller to respect the rights of data subjects

☐ Assist the Controller with security and other data protection compliance

☐ Assist the Controller with the Information Commissioner requirements

☐ Delete or return data at the end of the contract

☐ Details of processing activities to be made available to the Controller

☐ Any legal requirements for disclosure to a third party by the Processor to be notified

Appendix B: Processing Special Categories and Criminal Convictions Data

B.1 Article 9(1) of the GDPR prohibits the processing of special categories of personal data unless a condition in Article 9(2) is met, such as for reasons of substantial public interest (see Part 2, Schedule 1 of the DPA 2018). For the Foundation and Academy Trust, the processing of special categories of personal data ("sensitive processing") is only permitted where it is necessary for a function conferred by law or for government purposes, and it is necessary for reasons of substantial public interest. There is a further requirement that this condition will only be met if the sensitive processing is carried out in accordance with this policy. Foundation and Academy Trust staff must, therefore, have regard to this policy when carrying out sensitive processing on behalf of the authority and when acting in its capacity as Controller of personal data.

B.2 Personal data about criminal offences and convictions are dealt with separately in Article 10 of the GDPR. The DPA 2018 indicates that the processing of such data meets the requirements of Article 10 only if it meets a condition set out in Parts 1, 2, or 3 of Schedule 1. Where the processing of such data is carried out with reliance on a condition in Parts 1, 2, or 3 of Schedule 1, which requires the controller to have an appropriate policy in place when the processing is carried out, the Foundation and Academy Trust must have regard to this policy.

B.3 Below is how we demonstrate compliance with the data protection principles:

a) Lawfulness, fairness, and transparency: The lawfulness of the Foundation and Academy Trust's processing is derived from its official functions as a non-departmental public body. Transparency is provided using a layered approach. Detailed information about how both entities use personal data, including special category data, is published in the Privacy Policy on our website. These notices make it clear what data must be provided and why the data is needed.

b) Purpose limitation: Both entities only process personal data when permitted to do so by law. Any use of this data for a non-Foundation or Academy Trust function must have a specific lawful basis and be compatible with data protection obligations; the processing must, therefore, be proportionate and necessary.

c) Data minimisation: Each school has an application form or process to ensure they only collect the information necessary to determine entitlement or deliver services. Data subjects will not be asked to answer questions and provide information that is not required. Additionally, internal guidance, training, and policies mandate that staff use only the minimum amount of data required to enable specific tasks to be completed. Where the processing is for research and analysis purposes, wherever possible, this is done using anonymised or de-identified data sets.

d) Accuracy: Providing complete and accurate information is required when applying to the Academies. Data subjects are required to notify the Foundation and/or Academy Trust of relevant changes in their circumstances, such as changes of address or criminal record. Where permitted by law, and when it is reasonable and proportionate to do so, the Foundation and/or Academy Trust may check this information with other organisations, for example, the Home Office, the Police, or HMRC. If a change is reported by a data subject to one function at the Foundation/Academy Trust, whenever possible, this is also used to update other functions, both to improve

accuracy and avoid the data subject having to report the same information multiple times.

e) Storage limitation: The Foundation and Academy Trust has a comprehensive set of retention policies in place which are published on the website.

f) Integrity and confidentiality: Both entities have a range of security standards and policies based on industry best practices and government requirements to protect information from relevant threats. We apply these standards whether the data is being processed by our own staff or by a processor on our behalf.

B.4 All staff handling Foundation and Academy Trust information are security cleared and required to complete training on the importance of security and how to handle information appropriately.

Appendix C: Data Breach Process

C.1 A data security breach includes both confirmed and suspected incidents. An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity, or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the Foundation and/or Academy Trust's information assets and/or reputation.

C.2 An incident includes but is not restricted to the following: loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g., loss of laptop, USB stick, iPad/tablet device, or paper record); system failure; unauthorised use of/access to or modification of data or information systems; attempts (failed or successful) to gain unauthorised access to information or IT system(s); unauthorised disclosure of sensitive/confidential data; website defacement; hacking attack; human error and unforeseen circumstances; 'blagging' offences where information is obtained by deceiving the organisation that holds it.

C.3 All data security breaches shall be logged on the GDPR Sentry system as soon as they are discovered. Once logged, the Data Protection Officer/Risk and Compliance team will assess: The extent of the breach; the risks to the data subjects and organisation; any security measures in place that will protect the information; immediate actions to mitigate the risk to the organisation and data subjects as well as strategic measures that can help prevent future breaches.

C.4 Unless the Data Protection Officer concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office (ICO) within 72 hours of the breach having been discovered unless a delay can be justified. The ICO report must be produced via the GDPR Sentry system, which contains all the relevant information the ICO needs to know.

C.5 If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals, then the Data Protection Officer shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

C.6 Following an investigation, any measures recommended by the Data Protection Officer will go through the relevant governing body before implementation.

Appendix D: Subject Access Requests

D.1 Anybody who makes a request to see any personal information held about them by the Foundation and/or Academy Trust is making a subject access request. All information relating to the individual, including that held in electronic or manual files, should be considered for disclosure if they constitute a “filing system”.

D.2 The individual’s full subject access right is to know: whether personal data about them are being processed; the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipients to whom their personal data have been or will be disclosed; the envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored; the existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing; the right to lodge a complaint with the Information Commissioner’s Office; where the personal data are not collected from the individual, any available information as to their source; details of the safeguards in place for any transfers of their data to locations outside the UK.

D.3 All requests should be logged on the GDPR Sentry system by the Data Protection Lead (DPL) or the individual who received the request. The individual who receives the request must not redirect the requester; they must acknowledge receipt of the request themselves in the first instance. The Data Protection Officer will work with the DPL to respond to the request. The request must be dealt with in full without delay and within one month of receipt at the latest.

D.4 The parent of the data subject can request access to their child’s data. However, if the data subject is competent to exercise their data protection rights (which usually means they are over the age of 13), they must make the request and provide consent.

D.5 Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances, the Foundation and/or Academy Trust must have written evidence that the individual has authorised the person to make the application, and the DPL must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

D.6 Access to records will be refused in instances where an exemption applies. For example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

D.7 A subject access request can be submitted verbally or in writing. The DPO/DPL may ask for any further information reasonably required to locate the information.

D.8 An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

D.9 All files must be reviewed by the Data Protection Officer or the school DPL before any disclosure takes place.

D.10 Where all the data in a document cannot be disclosed, a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, along with the reason why the document was altered.

Appendix E: Freedom of Information Requests

E.1 King Edward VI Academy Trust Birmingham (the "Academy Trust") and its Academies are subject to the Freedom of Information Act 2000 ("FOI") as a public authority and, as such, must comply with any requests for information in accordance with the principles laid out in the Act.

E.2 The Schools of King Edward VI in Birmingham (the "Foundation") is a registered charity and not owned by a public authority. Therefore, it is not subject to the Freedom of Information Act 2000.

E.3 Any request for information from the Academy Trust is technically a request under the FOI, whether the individual making the request mentions the FOI. However, the ICO has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act.

E.4 All non-routine requests and those specifically that mention FOI must be logged on the GDPR Sentry System as soon as they are made. The DPO will work with the DPL at a school level to assess the request and produce an appropriate response.

E.5 The Academy Trust must respond as soon as possible and, in any event, within 20 working days of the date of receipt of the request. For the Trust, a "working day" is one in which pupils are in attendance, subject to an absolute maximum of 60 calendar days to respond.

E.6 The first stage in responding is to determine whether the Academy "holds" the information requested. The Academy will hold the information if it exists in computer or paper format. Some requests will require the Academy to take information from different sources and manipulate it in some way. Where this would take minimal effort, the Academy is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested and offered the opportunity to refine their request. For example, if a request required the Academy to add up totals in a spreadsheet and release the total figures, this would be information "held" by the Academy. If the Academy would have to go through several spreadsheets and identify individual figures and provide a total, this is likely not to be information "held" by the Academy, depending on the time involved in extracting the information.

E.7 The second stage is to decide whether the information can be released or whether one of the exemptions set out in the Act applies to the information. The DPO will work with the DPL using ICO guidance to determine whether information can be released.

E.8 The DPO/Risk and Compliance team will work with the DPL to produce an appropriate response. The response must include whether we hold the information, which exemptions have been applied and why as well as detailing their rights for internal and ICO review.

E.9 The requester has the right to ask for an internal review. Depending on who produced the response, the DPO or a member of the SLT will conduct the review. After an internal review, the requester also has the right to ask the ICO to complete an independent review.

Appendix F: Data Retention Schedule

This guidance is based on industry standards provided by the Information and Records Management Society.

1.1	Management of the Governing Body				
	Basic file description	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
1.1.1	Instruments of government		For the life of the school	Consult archives before disposal	
1.1.2	Trusts and endowments		Life of the Trust or Endowment + 6 Years	Consult archives before disposal	
1.1.3	Records relating to the election of parent and staff governors not appointed by the governors		Date of election + 6 months	Secure disposal	Yes
1.1.4	Records relating to the appointment of co-opted governors		Provided that the decision has been recorded in the minutes, the records relating to the appointment can be destroyed once the co-opted governor has finished their term of office (except where there have been allegations concerning children). In this case, retain for 25 years.	Secure disposal	Yes
1.1.5	Records relating to the election of chair and vice chair		Once the decision has been recorded in the minutes, the records relating to the election can be destroyed	Secure disposal	Yes

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
1.1.6	Scheme of delegation and terms of reference for committees		Until superseded or whilst relevant [we may to retain these records for reference purposes in case decisions need to be justified]	These could be offered to the archives if appropriate	
1.1.7	Meetings schedule		Current year	Standard disposal	
1.1.8	Agendas - principal copy		One copy should be retained with the master set of minutes. All other copies can be disposed of	Consult archives before disposal	Potential
1.1.9	Minutes - principal set (signed)		Date of the meeting + a minimum of 10 years	Consult archives before disposal	Potential
1.1.10	Reports made to the governors' meeting which are referred to in the minutes		Although generally kept for the life of the organisation, they are only required to be made these available for 10 years from the date of the meeting	Consult archives before disposal	Potential
1.1.11	Register of attendance at Full governing board meetings		Date of last meeting in the book + 6 years	Secure disposal	Yes
1.1.12	Agendas - additional copies		Date of meeting	Secure disposal	
1.1.13	Records relating to Governor Monitoring Visits		Date of the visit + 3 years	Secure disposal	Yes
1.1.14	Reports submitted to the DfE		Date of report + 10 years	Secure disposal	

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
1.1.15	All records relating to the conversion of schools to Academy status		For the life of the organisation	Consult archives before disposal	
1.1.16	Records relating to complaints made to and investigated by the governing body or head teacher		Date complaint resolved + 3 years then review. If the complaint relates to negligence or safeguarding then date the complaint resolved + 15 years. If the complaint relates to child sexual abuse then the complaint resolved + 75 years (this retention period will be reviewed once the government and the ICO have issued guidance about the implementation of the IICSA recommendations)	Secure disposal	Yes
1.1.17	Correspondence sent and received by the governing body or head teacher		General correspondence should be retained for current year + 3 years	Secure disposal	Potential
1.1.18	Action plans created and administered by the governing body		Until superseded or whilst relevant	Secure disposal	
1.1.19	Policy documents created and administered by the governing body		6 years then review. Upon review, consideration should be given to ongoing retention of safeguarding and child protection policies or other pupil related issues such as exclusion.		

1.2 Governor Management					
	Basic file description	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
1.2.1	Records relating to the appointment of a clerk to the governing body		Date on which clerk appointment ceases + 6 years	Secure disposal	Yes
1.2.2	Records relating to the terms of office of serving governors, including evidence of appointment		Date appointment ceases plus 6 years except where there have been allegations concerning children. In this case retain for 25 years.	Secure disposal	Yes
1.2.3	Records relating to governor declaration against disqualification criteria		Date appointment ceases + 6 years	Secure disposal	Yes
1.2.4	Register of business interests		Date appointment ceases + 6 years	Secure disposal	Yes
1.2.5	Governors Code of Conduct		This is expected to be a dynamic document; one copy of each version should be kept for the life of the organisation	Send to archive	
1.2.6	Records relating to the training required and received by Governors		Date Governor steps down + 6 years	Secure disposal	Yes
1.2.7	Records relating to the induction programme for new governors		Date appointment ceases + 6 years	Secure disposal	Yes
1.2.8	Records relating to DBS checks carried out on clerk and members of the governing body		Date of DBS check + 6 months.	Secure disposal	Yes

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
1.2.9	Governor personnel files		Date appointment ceases plus 6 years except where there have been allegations concerning children. In this case retain for 25 years	Secure disposal	Yes
1.2.10	Video recordings of Governors		3 months following recording except when videos are used for training purposes where it is held as long as is needed	Secure disposal	Yes

2 Management of the School

This section contains retention periods connected to the processes involved in managing the school, including Human Resources, Financial Management, Payroll, and Property Management.

2.1	Head Teacher and Senior Management Team				
	Basic file description	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
2.1.1	Log books of activity in the school maintained by the Head Teacher		Date of last entry in the book + minimum of 6 years, then review	These could be of permanent historical value and should be offered to the archive if appropriate	Potential
2.1.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies		Date of the meeting + 3 years then review	Secure disposal	Potential
2.1.3	Reports created by the Head Teacher or the Management Team		Date of the report + 3 years then review	Secure disposal	Potential
2.1.4	Records created by head teachers, deputy head teachers, heads of year, and other members of staff with administrative responsibilities which do not fall under any other category		Current academic year + 3 years then review	Secure disposal	
2.1.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities		Date of correspondence + 3 years	Secure disposal	Potential
2.1.6	Professional development plans		Life of the plan or plan superseded + 6 years	Secure disposal	Potential

	Basic file descriptions	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal Information
2.1.7	School development plans		Life of plan or until plan superseded + 3 years. If major changes are made to the plan then an archive copy of previous plans should be retained.	Secure disposal	

2.2 Operational Administration

	Basic file descriptions	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
2.2.1	General file series which do not fit under any other category		Current year + 5 years, then review	Secure disposal	Potential
2.2.2	Records relating to the creation and publication of the school brochure or prospectus		Current year + 3 years. Schools should consider archiving one copy for historical reasons	The school could preserve a copy for their archive otherwise, standard disposal	
2.2.3	Records relating to the creation and distribution of circulars to staff, parents or pupils		Current academic year + 1 year	Standard disposal	
2.2.4	School Privacy Notice which is sent to parents as part of GDPR compliance		Life of the privacy notice/until the privacy notice is superseded plus 6 years		
2.2.5	Consents relating to school activities as part of GDPR compliance (for example, consent to be sent circulars or mailings)		Consents should be retained for as long as the consent is relied on.	Secure disposal	Yes
2.2.6	Newsletters and other items with a short operational use		Current year + 1 year	Standard disposal	
2.2.7	Visitor management systems (including electronic systems, visitor books, and signing-in sheets)		6 years	Secure disposal	Yes
2.2.8	Walking bus registers		Date of register + 3 years. If there is an incident requiring an accident report, the register will be submitted with the accident report and kept for the period of time required for accident reporting.	Secure disposal	Yes

2.3 Human Resources					
	Basic file description	**Statutory provisions [operational]**	**Retention period**	**the administrative life information of the record**	**Personal Information**
Recruitment					
2.3.1	All records leading up to the appointment of a headteacher		Unsuccessful attempts. Date of appointment + 6 months. Add to personnel file and retain until the end of appointment + 6 years, except in cases of negligence or claims of child abuse, then at least 15 years	Secure disposal	Yes
2.3.2	All records leading up to the appointment of a member of staff/governor - unsuccessful candidates		Date of appointment of successful candidate + 6 months	Secure disposal	Yes
2.3.3	Pre-employment vetting information - DBS Checks - successful candidates	DBS Update Service Employer Guide; Keeping Children Safe in Education, (Statutory Guidance from DoE) Sections 73, 74	Schools do not have to keep copies of DBS certificates in order to fulfil the duty of maintaining the single central record. When a school chooses to retain a copy, there should be a valid reason for doing so and it should not be kept for longer than six months. When the information is destroyed, it must be done securely. Once a recruitment (or other relevant) decision has been made, we do not keep certificate information (e.g. DBS number) for any longer than is necessary. This retention will allow for the consideration and resolution of any disputes or complaints,	Secure disposal	Yes

			or be for the purpose of completing safeguarding audits. If the school disposes of the certificate the following information should be retained in line with the DBS Code of Practice: Retain the following after the certificate is destroyed - 1. The date of issue of a disclosure; 2. The name of the subject; 3. The type of the disclosure requested; the position for which the Disclosure was requested; 4. The unique reference number of the Disclosure; 5. The details of the recruitment decision taken.		
2.3.4	Forms of proof of identity collected as part of the process of checking “portable” enhanced DBS disclosure		Where possible, this process should be carried out using the online system. If it is necessary to take a copy of the documentation, then it should be retained on the staff personal file	Secure disposal	Yes
2.3.5	Pre-employment vetting information - Evidence proving the right to work in the United Kingdom - successful candidates	An Employer’s Guide to Right to Work Checks [Home Office]	Where possible, these copies of documents should be added to the Staff Personal File, but if they are kept separately, then the Home Office requires that the documents are kept for termination of employment plus not less than 2 years	Secure disposal	Yes

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
Operational Staff Management					
2.3.6	Staff personnel file	Limitation Act (Section 2)	Termination of employment + 6 years	Secure disposal	Yes
2.3.7	Annual appraisal/assessment records		Current year + 6 years	Secure disposal	Yes
2.3.8	Sickness absence monitoring		Sickness records are categorised as sensitive data. There is a legal obligation under statutory sickness pay to keep records for sickness monitoring. Sickness records should be kept separate from accident records. Fit notes should be kept by line managers for current year + 3 years. Records of sick pay should be kept for current year + 6 years.	Secure disposal	Yes
2.3.9	Staff training - where the training leads to continuing professional development		Length of time required by the professional body	Secure disposal	Yes
2.3.10	Staff training - except where dealing with children, e.g. first aid or health and safety		This should be retained on the personnel file [see 2.3.6 above]	Secure disposal	Yes
2.3.11	Staff training - where the training relates to children (e.g. safeguarding or other child-related training)		Date of the training + 40 years	Secure disposal	Yes

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
2.3.12	Staff Biometric information		Until Staff member withdraws consent	Secure disposal	Yes
2.3.13	Video recordings of Staff		3 months of recording except when videos are used for training where it is held as long as is needed	Secure disposal	Yes
Disciplinary and Grievance Processes					
Where schools are in any doubt as to which categories disciplinary records fall under, then HR or legal advice should be sought.					
2.3.14	Records relating to any allegation of a child protection nature against a member of staff	"Keeping children safe in education Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to interagency working to safe-guard and promote the welfare of children"	Until the persons normal retirement age or 10 years from the date of the allegation, whichever is longer, then review.	Secure disposal. These records must be shredded	Yes

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
Disciplinary and Grievance Processes					
2.3.15	Disciplinary proceedings:				Yes
	Written warning		Date of warning + 1 year	Secure disposal [If warnings are placed on personal files, then they must be weeded from the file).	
	Final written warning		Date of warning + 2 years		
	Final warning		Date of warning + 18 months		
	Case not found		If the incident is child protection related, then see 2.3.14 otherwise dispose of at the conclusion of the case	Secure disposal	

Note:
The ACAS code of practice on disciplinary and grievance procedures recommends that the employee should be told how long a disciplinary warning will remain current. However, this does not mean that the data itself should be destroyed at the end of the set period.

Any disciplinary proceedings data will be a record of an important event in the course of the employer's relationship with the employee. Should the same employee be accused of similar misconduct five years down the line, and them defend him- or herself by saying, "I would never do something like that", reference to the earlier proceedings may show that the comment should not be given credence. Alternatively, if the employee were to be dismissed for some later offence and then claim at tribunal that they had "fifteen years of unblemished service", the record of the disciplinary proceedings would be effective evidence to counter this claim.

Employers should, therefore, be careful not to confuse the expiry of a warning for disciplinary purposes with a requirement to destroy all reference to its existence in the personnel file. One danger is that the disciplinary procedure itself often gives the impression that, at the end of the effective period for the warning, the warning will be "removed from the file". This or similar wording should be changed to make it clear that, while the warning will not remain active in relation to future disciplinary matters, a record of what has occurred will be kept.

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
Payroll and Pensions					
2.3.16	Absence record		Current year + 3 years	Secure disposal	Yes
2.3.17	Batches	Taxes Management Act Income and Corporation Taxes Act	Current year + 6 years	Secure disposal	Yes
2.3.18	Bonus sheets	Taxes Management Act Income and Corporation Taxes Act	Current year + 3 years	Secure disposal	Yes
2.3.19	Car allowance claims	Taxes Management Act Income and Corporation Taxes Act	Current year + 3 years	Secure disposal	Yes
2.3.20	Car loans	Taxes Management Act Income and Corporation Taxes Act	Completion of loan + 6 years	Secure disposal	Yes
2.3.21	Car mileage output	Taxes Management Act Income and Corporation Taxes Act	Current year + 6 years	Secure disposal	Yes

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
2.3.22	Elements		Current year + 2 years	Secure disposal	Yes
2.3.23	Income tax form P60		Current year + 6 years.	Secure disposal	Yes
2.3.24	Insurance	Taxes Management Act Income and Corporation Taxes Act	Current year + 6 years	Secure disposal	Yes
2.3.25	Maternity payment		Current year + 3 years	Secure disposal	Yes
2.3.26	Members allowance register	Taxes Management Act Income and Corporation Taxes Act	Current year + 6 years	Secure disposal	Yes
2.3.27	National Insurance schedule of payments	Taxes Management Act Income and Corporation Taxes Act	Current year + 6 years	Secure disposal	Yes
2.3.28	Overtime	Taxes Management Act Income and Corporation Taxes Act	Current year + 3 years	Secure disposal	Yes
2.3.29	Part time fee claims	Taxes Management Act Income and Corporation Taxes Act	Current year + 6 years	Secure disposal	Yes

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
2.3.30	Pay packet receipt by employee		Current year + 2 years	Secure disposal	Yes
2.3.31	Payroll awards		Current year + 6 years	Secure disposal	Yes
2.3.32	Payroll - gross/net week	Taxes Management Act Income and Corporation Taxes Act	Current year + 6 years	Secure disposal	Yes
2.3.33	Payroll reports	Taxes Management Act Income and Corporation Taxes Act	Current year + 6 years	Secure disposal	Yes
2.3.34	Payslips - copies	Taxes Management Act Income and Corporation Taxes Act	Current year + 6 years	Secure disposal	Yes
2.3.35	Pension payroll	Taxes Management Act Income and Corporation Taxes Act	Current year + 6 years	Secure disposal	Yes
2.3.36	Personal bank details		Until superseded + 3 years If employment ceases, then end of employment + 6 years	Secure disposal	Yes
2.3.37	Sickness records		Current year + 3 years	Secure disposal	Yes

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
2.3.38	Staff returns		Current year + 3 years	Secure disposal	Yes
2.3.39	Superannuation adjustments	Taxes Management Act Income and Corporation Taxes Act	Current year + 6 years	Secure disposal	Yes
2.3.40	Superannuation reports	Taxes Management Act Income and Corporation Taxes Act	Current year + 6 years	Secure disposal	Yes
2.3.41	Tax forms P6/P11/ P11D/P35/P45/P46/ P48	The minimum requirement - as stated in Inland Revenue Booklet 490 - is for at least 3 years after the end of the tax year to which they apply. Originals must be retained in paper/ electronic format. It is a corporate decision to retain for current year + 6 years. Employees should retain records for 22 months after current tax year	Current year + 6 years	Secure disposal	Yes
2.3.42	Time sheets/clock cards/flexitime		Current year + 3 years	Secure disposal	Yes

2.4	Health and Safety				
	Basic file description	**Statutory provisions [operational]**	**Retention period**	**Action at the end of the administrative life of the record**	**Personal information**
2.4.1	Health and safety policy statements		Life of policy + 6 years	Secure disposal	
2.4.2	Health and safety risk assessments		Life of risk assessment + 3 years	Secure disposal	
2.4.3	Accident reporting records relating to individuals who are over 18 years of age at the time of the incident	Social Security (Claims and Payments) Regulations Regulation 25. Social Security administration Act Section 8. Limitation Act SI No 628 Social Security (Claims and Payments) Regulations SI No 1968 revokes all but Part 1 of SI 1979 No 628 Social Security (Claims and Payments) Amendment (No 30 Regulations SI No 2113 Allows the information to be kept electronically	Date of last entry in the accident book + 3 years but if there is possibility of a negligence allegation then date of incident + 15 years or date of settlement + 6 years	Secure disposal	Yes

	Basic file description	Statutory provisions [operational]	Retention period	Action at the end of the administrative life of the record	Personal information
2.4.4	Accident reporting records relating to individuals who are under 18 years of age at the time of the incident	Social Security (Claims and Payments) Regulations Regulation 25. Social Security Administration Act Section 8. Limitation Act Social Security (Claims and Payments) Regulations. SI No 628 Social Security (Claims and Payments) Regulations SI No 1968 Revokes all but Part 1 of SI 1979 No 628 Social Security Administration Act Section 8. Social Security (Claims and Payments) Amendment (No 30 Regulations SI No 2113 Allows the information to be kept electronically	The official Accident Book must be retained for 3 years after the last entry in the book. The book may be in paper or electronic format The incident reporting form may be retained as below 2.4.5. Do not keep completed entries in the book. They must be removed and kept in a locked location.	Secure disposal	Yes
2.4.5	Records relating to any reportable death, injury, disease, or dangerous occurrence (RIDDOR). For more information, see http://www.hse.gov.uk/RIDDOR/	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations SI No 1471 Regulation 12(2)	Date of incident + 3 years provided that all records relating to the incident are held on personnel file. See 2.4.4	Secure disposal	Yes

	Basic file description	Statutory provisions [operational]	Retention period	Action at the end of the administrative life of the record	Personal information
2.4.6	Control of Substances Hazardous to Health (COSHH)	Control of Substances Hazardous to Health Regulations. SI No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	COSHH sheets should be kept whilst the substance is in use + 6 years COSHH policy documents should be kept until the policy is superseded + 6 years	Secure disposal	
2.4.7	Process of monitoring of areas where employees and persons are likely to have come into contact with asbestos	Control of Asbestos at Work Regulations SI 1012 No 632 Regulation 19	Last action + 40 years	Secure disposal	
2.4.8	Process of monitoring of areas where employees and persons are likely to have come into con- tact with radiation. Maintenance records or controls, safety features and PPE: Dose assessment and recording	The Ionising Radiation Regulations. SI 2017 No 1075 Regulation 11 As amended by SI No 390 Personal Protective Equipment (Enforcement) Regulations	2 years from the date on which the examination was made and that the record includes the condition of the equipment at the time of the examination. To keep the records made and maintained or a copy of these records until the person to whom the record relates has or would have attained the age of 75 years but in any event for at least 30 years from when the record was made	Secure disposal	
2.4.9	Fire Precautions log books		Current year + 6 years	Secure disposal	2.4.9

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
2.4.10	Health and safety file to show current state of building, including all alterations (wiring, plumbing, building works, etc.), to be passed on in the case of change of ownership		Pass to new owner on sale or transfer of building. Copy to be kept in archive	Copies of plans to be kept in archive upon completion of projects.	

2.5	Financial Management				
	Basic file description	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
Risk Management and Insurance					
2.5.1	Employer's Liability Insurance Certificate		Closure of the school + 40 years [May be kept electronically]	Secure disposal. To be passed to the Local Authority if the school closes	
Asset Management					
2.5.2	Inventories of furniture and equipment		Current year + 6 years	Secure disposal	
2.5.3	Burglary, theft and vandalism report forms		Current year + 6 years	Secure disposal	
Accounts and Statements (including budget management)					
2.5.4	Annual accounts		Current year + 6 years	Secure disposal	
2.5.5	Loans and grants managed by the school		Date of last payment on loan + 6 years if the loan is under 10,000 or date of last payment on loan + 12 years if the loan is over 10,000	Secure disposal	
2.5.6	All records relating to the creation and management of budgets, including the annual budget statement and background papers		Life of the budget + 3 years	Secure disposal	
2.5.7	Invoices, receipts, order books and requisitions, delivery notices		Current financial year + 6 years	Secure disposal	

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
2.5.8	Records relating to the collection and banking of monies		Current financial year + 6 years	Secure disposal	
2.5.9	Records relating to the identification and collection of debt		Final payment of debt + 6 years	Secure disposal	
Pupil Finance					
2.5.10	Student Grant applications		Current year + 3 years	Secure disposal	Yes
2.5.11	Pupil Premium Fund records		Date pupil leaves the provision + 6 years	Secure disposal	Yes
Contract Management					
2.5.12	All records relating to the management of contracts under seal	Limitation Act	Last payment on the contract + 12 years or end of contract + 12 years, whichever is the longer	Secure disposal	
2.5.13	All records relating to the management of contracts under signature	Limitation Act	Last payment on the contract + 6 years or end of contract + 6 years whichever is the longer	Secure disposal	
2.5.14	Records relating to the monitoring of contracts		Life of contract + 6 or 12 years	Secure disposal	
School Fund					
2.5.15	School Fund - Cheque books		Current year + 6 years	Secure disposal	
2.5.16	School Fund - Paying in books		Current year + 6 years	SECURE DISPOSAL	

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
2.5.17	School Fund - Ledger		Current year + 6 years	SECURE DISPOSAL	
2.5.18	School Fund - Invoices		Current year + 6 years	SECURE DISPOSAL	
2.5.19	School Fund - Receipts		Current year + 6 years	SECURE DISPOSAL	
2.5.20	School Fund - Bank statements		Current year + 6 years	SECURE DISPOSAL	
2.5.21	School Fund - Journey Books		Current year + 6 years	SECURE DISPOSAL	
School Meals Management					
2.5.22	Free school meals registers (where the register is used as a basis for funding)		Current year + 3 years	SECURE DISPOSAL	Yes
2.5.23	School meals registers		Current year + 3 years	SECURE DISPOSAL	Yes
2.5.24	School meals summary sheets		Current year + 3 years	SECURE DISPOSAL	Yes

2.6	Property Management				
	Basic file description	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
2.6.1	Title deeds of properties belonging to the school		These should follow the property unless the property has been registered with the Land Registry		
2.6.2	Plans of property belonging to the school		These should be retained whilst the building belongs to the school and should be passed on to any new owners if the building is leased or sold. See 2.4.10		
2.6.3	Leases of property leased by or to the school		Expiry of lease + 6 years	SECURE DISPOSAL	
2.6.4	Records relating to the letting of school premises		Current financial year + 6 years	SECURE DISPOSAL	
Maintenance					
2.6.5	All records relating to the maintenance of the school carried out by contractors		These should be retained whilst the building belongs to the school and should be passed on to any new owners if the building is leased or sold. See 2.4.10	SECURE DISPOSAL	
2.6.6	All records relating to the maintenance of the school carried out by school employees, including maintenance log books		These should be retained whilst the building belongs to the school and should be passed on to any new owners if the building is leased or sold. See 2.4.10	SECURE DISPOSAL	

3. Pupil Management

This section contains retention periods connected to the processes involved in managing a pupil's journey through school, including the admissions process.

3.1 Admissions Process					
	Basic file description	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
3.1.1	All records relating to the creation and implementation of the School Admissions Policy	School Admissions Code: Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals Panels	Life of the policy + 3 years, then review	SECURE DISPOSAL	
3.1.2	Admissions - if the admission is successful	School Admissions Code: Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators, and admission appeals Panels	Date of admission + 1 year	SECURE DISPOSAL	Yes
3.1.3	Admissions - if the appeal is unsuccessful	School Admissions Code: Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators, and admission appeals Panels	Resolution of case + 1 year	SECURE DISPOSAL	Yes
3.1.4	Register of Admissions	School Admissions Code: Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators, and admission appeals panels	Every entry in the admission register must be preserved for three years after the date on which the entry was made	REVIEW Schools may wish to consider keeping the admission register permanently as an archive record as often schools receive enquiries from past pupils to confirm the dates they attended the school or to transfer these records to the appropriate Archives Service	

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
3.1.5	Admissions - Secondary Schools - Casual		Current year + 1 year	SECURE DISPOSAL	Yes
3.1.6	Proofs of address supplied by parents as part of the admissions process	School Admissions Code: Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals Panels	Current year + 1 year	SECURE DISPOSAL	Yes
3.1.7	Supplementary information form including additional information such as religion, medical conditions, etc. :				
3.1.7.1	For successful admissions		This information should be added to the pupil file	SECURE DISPOSAL	
3.1.7.2	For unsuccessful admissions		Until appeals process is completed (GDPR)	SECURE DISPOSAL	

3.2 Pupil's Educational Record					
	Basic file description	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
3.2.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005:				Yes
3.2.1.1	Primary	The Education (Pupil Information) (England) Regulations SI No. 1437 As amended by SI 2018 No 688	Retain whilst the child remains at the primary school	The file should follow the pupil when they leave the primary school. This will include: • To another primary school • To a secondary school • To a pupil referral unit	
3.2.1.2	Secondary	Limitation Act (Section 2)	Date of birth of the pupil + 25 years	REVIEW	
3.2.2	Examination Results - pupil copies:				Yes
3.2.2.1	Public		This information should be added to the pupil file	All uncollected certificates should be returned to the examination board after reasonable attempts to contact the pupil have failed	
3.2.2.2	Internal		This information should be added to the pupil file		
3.2.3	Child protection information held on pupil file	"Keeping Children Safe in Education: Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL These records must be shredded	Yes

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
3.2.4	Child protection information held in separate files	"Keeping children safe in education: Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	DOB of the child + 25 years, then review. This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL These records must be shredded	Yes

3.3 Attendance					
Basic file description		**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
3.3.1	Attendance Registers	School Attendance: Departmental advice for maintained schools, Academies, independent schools, and local authorities	Every entry in the attendance register must be preserved for a period of 6 years after the date on which the entry was made. Every back up copy of the register is to be preserved for 6 years after the end of the school year to which it relates.	Secure disposal	Yes
3.3.2	Correspondence relating to any absence (authorised or unauthorised)	Education Act Section 7	Current academic year +2 years	Secure disposal	
3.3.3	Special Educational Needs files, reviews and Individual Education Plans	Children and Family's Act; Special Educational Needs and Disability Act Section 14	Date of birth of the pupil + 25 years	Secure disposal	Yes

4. Curriculum and Extra Curricular Activities

This section contains retention periods connected to the processes involved in managing the curriculum and extra-curricular activities.

4.1 Statistics and Management Information

	Basic file description	Statutory provisions	Retention period [operational]	Action at the end of the administrative life of the record	Personal information
4.1.1	Curriculum returns		Current year + 3 years	Secure disposal	No
4.1.2	Examination Results (school's copy)		Current year + 6 years	Secure disposal	Yes
4.1.2.1	SATS records:				Yes
4.1.2.2	Results		The SATS results should be recorded on the pupils educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	Secure disposal	
4.1.2.3	Examination Papers		The examination papers should be kept until any appeals/validation process is complete	Secure disposal	
4.1.3	Published Admission Number (PAN) Reports		Current year + 6 years	Secure disposal	Yes
4.1.4	Value Added and Contextual Data		Current year + 6 years	Secure disposal	Yes
4.1.5	Self-evaluation forms:				
4.1.5.1	Internal moderation		Academic year plus 1 academic year	Secure disposal	Yes
4.1.5.2	External moderation		Until superseded	Secure disposal	Yes

4.2 Implementation of Curriculum					
	Basic file description	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
4.2.1	Schemes of work		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or secure disposal	
4.2.2	Timetable		Academic year + 1 year		
4.2.3	Class record books		Academic year + 1 year		
4.2.4	Mark books		Academic year + 1 year		
4.2.5	Record of homework set		Academic year + 1 year		
4.2.6	Pupil's work		Where possible, the pupil's work should be returned to the pupil at the end of the academic year. If this is not the school's policy then current year + 1 year	Secure disposal	

4.3 School visits					
	Basic file description	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
4.3.1	Parental consent forms for school visits where there has been no major incident		Conclusion of the trip. Although the consent forms could be retained for date of birth + 25 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time	Secure disposal	Yes
4.3.2	Parental permission slips for school visits- where there has been a major incident	Limitation Act (Section 2)	Date of birth of the pupil involved in the incident + 25 years. The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	Secure disposal	Yes

4.4	School Support Organisations				
	Basic file description	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
Family Liaison Officers and Home School Liaison Assistants					
4.4.1	Day books		Current year + 2 years then review	Secure disposal	Yes
4.4.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency		Whilst child is attending school and then destroy	Secure disposal	Yes
4.4.3	Referral forms		While the referral is current	Secure disposal	Yes
4.4.4	Contact data sheets		Current year, then review. If contact is no longer active, then destroy	Secure disposal	Yes
4.4.5	Contact database entries		Current year, then review. If contact is no longer active, then destroy	Secure disposal	Yes
4.4.6	Group registers		Current year + 2 years	Secure disposal	Yes
Parent Teacher Associations and Old Pupils Associations					
4.4.7	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations		Current year + 6 years then review	Secure disposal	

5. Central Government and Local Authority

This section covers records created in the course of interaction between the School and the Local Authority

5.1	Local Authority				
	Basic file description	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
5.1.1	Secondary Transfer Sheets (primary)		Current year + 2 years	Secure disposal	Yes
5.1.2	Attendance returns		Academic year + 1 year	Secure disposal	Yes
5.1.3	School census returns		Current year + 5 years	Secure disposal	
5.1.4	Circulars and other information sent from the local authority		Operational use	Secure disposal	

5.2	Central Government				
	Basic file description	**Statutory provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**	**Personal information**
5.2.1	OFSTED reports and papers where a physical copy is held		Life of the report, then review	Secure disposal	
5.2.2	Returns made to central government		Current year + 6 years	Secure disposal	
5.2.3	Circulars and other information sent from central government		Operational use	Secure disposal	

F.1 When a document is at the end of its retention period, it should either be destroyed via confidential waste or deleted electronically with IT support. The following guidance should be followed: https://www.gov.uk/guidance/data-protection-in-schools/record-keeping-and-management

F.2 When deciding about an individual document not covered by these retention periods, consider whether it has come to the end of its usefulness and whether it is of any historical importance.

F.3 The Foundation maintains a permanent archive of pupils who have attended a school of the Foundation. This archive comprises of but is not limited to the pupil's address when they started at the school, date of birth, parents' occupations, and what type of place they had (such as a scholarship), together with the dates they started and finished as a pupil. The archive can be accessed by the archivist for research and other purposes, but not for marketing.

END.