THE SCHOOLS OF KING EDWARD VI IN BIRMINGHAM

In pursuit of educational excellence for all

KING EDWARD VI ACADEMY TRUST BIRMINGHAM

DATA PROTECTION POLICY & DATA PROCESSING PROCEDURES

Responsible Board	Academy Trust Board and Foundation Board
Policy Type	Central Foundation & Trust-Level Policy
Policy Owner	Risk and Compliance
Date Adopted	May 2022
Last Review Date	N/A – new policy
Next Review Date	April 2023
Version	1

1. Introduction

1.1 The Schools of King Edward VI in Birmingham (the 'Foundation') and the King Edward VI Academy Trust Birmingham (the 'Academy Trust') collects and uses certain types of personal information about staff, pupils, parents, and other individuals who come into contact with the Foundation and Academy Trust in order 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, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation ('GDPR') 2018, the Data Protection Act 2018 and other related legislation.

1.2 The 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 where the data is structured in some way that it is searchable based on specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is in a different physical location.

1.3 The appendices to this policy detail how data is processed, including the processing of special category and criminal conviction data. As well as the process to deal with data/information requests, retention periods and the data breach process.

1.4 This policy will be updated as necessary to reflect best practice, or changes in relevant legislation and shall be reviewed annually.

2. Personal Data

2.1 '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 sub-set 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.

2.2 Special category data is given enhanced protection and additional safeguards apply – please see Appendix B for more details.

2.3 Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

2.4 The Foundation and Academy Trust does 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 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).

3. Data Protection Principles

3.1 The Foundation and Academy Trust will adhere to the six data protection principles as outlined in the GDPR:

- personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met
- personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes
- personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed
- personal data shall be accurate and, where necessary, kept up to date
- personal data processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose/those purposes
- personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.2 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 the privacy notices which we issue
- 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.

4. Conditions for Processing

4.1 The individual has given consent that is specific to the processing activity, and that consent is informed, unambiguous and freely given.

4.2 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 with regards to entering a contract with the individual, at their request.

4.3 The processing is necessary for the performance of a legal obligation to which we are subject.

4.4 The processing is necessary to protect the vital interests of the individual or another.

4.5 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.

5. Use of Personal Data by the Foundation and Academy Trust

5.1 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.

Pupils

5.2 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, and photographs.

5.3 The data is used to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the school/academy is doing, together with any other uses normally associated with this provision in a school environment.

5.4 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 to 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 his/her academic progress and achievements

- Use photographs of pupils in accordance with the photograph policy.

Staff

5.5 The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks, occupational pensions, and photographs.

5.6 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.

5.7 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.

5.8 DBS 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.

5.9 Access to the DBS information is restricted to those 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

5.10 The Foundation and Academy Trust may hold personal information in relation to other individuals who have contact with its Academies, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

5.11 Any wish to limit or object to the uses to which personal data is to be 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.

6. Security of Personal Data

6.1 The Foundation and Academy Trust will take reasonable steps to ensure that members of staff 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.

6.2 Please refer to the IT policies for further details

7. Disclosure of Personal Data to Third Parties

7.1 The following list includes the most usual 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 relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

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

8. Confidentiality of Pupil Concerns

8.1 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 guardian, 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 a safeguarding purpose will be lawful because it will be in the substantial public interest.

9. Other Rights of Individuals

Right to object to processing

9.1 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

9.2 Where such an objection is made, it must be sent to the Data Protection Officer within 2 working days of receipt, and 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 for the establishment, exercise, or defence of legal proceedings.

9.3 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 rectification

9.4 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 to the Data Protection Officer within 2 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.

9.5 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 an appeal direct to the Information Commissioner.

9.6 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

9.7 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
- 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.

9.8 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

9.9 In the following circumstances, 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.

Right to restrict processing

9.10 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 provides 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 a request for this is made, it should be forwarded to the Data Protection Officer within 2 working days of receipt, and the Data Protection Officer will review and revert as necessary.

10. Contact and Linked Policies

10.1 If you have any questions regarding this policy, please contact Tim Hasker, Data Protection Officer for the Academy Trust, and Foundation via dataprotection@ske.uk.net

10.2 Linked 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 providing 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 approved certification should be recited in the agreement you have with the Processor.

A.3 To comply with the law, your agreement with the Processor must be 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; 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 security of data, co-operating in relation to your notification of breaches to the Information Commissioner's Office and data subjects, and with preparation of 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. The choice of 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 law of England and Wales or 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 law of England and Wales or law of EU or other member state

☐ Names of Processor and Controller details

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

☐ Processor can only act on instructions of Controller

☐ Duty of confidentiality for Processor's staff

☐ Processor to implement necessary security measures

☐ Only sub-contract with Controller's permission

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

☐ Assist the Controller with security and other data protection compliance

☐ Assist the Controller with Information Commissioner requirements

☐ Delete or return data at the end of the contract

☐ Details of processing activities to be made available to Controller

☐ Any legal requirements for disclosure to third party by 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, when it is 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 provides that the processing of such data meets the requirements of Article 10 only if it meets a condition set out in Part 1, 2 or 3 of Schedule 1. Where the processing of such data is carried out with reliance on a condition in Part 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 Detailed 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 the reason why 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 is required to have a specific lawful basis and it must 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 collects 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 require staff to use only the minimum amount of data required to enable specific tasks to be completed.

Where 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 practice 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 who 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 Office/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 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 which the ICO will need 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 him or her are being processed
- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipient 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 that received the request. 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 at the latest within one month of receipt.

D.4 The parent of the data subject can request access to their child's data, however, if the data subject is 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, 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 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 spread sheet and release the total figures, this would be information "held" by the Academy. If the Academy would have to go through several spread sheets 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 review will be conducted by the DPO or member of the SLT. After an internal review the requester also has the right to ask the ICO to complete an independent review.

Appendix F: Data Retention Periods

DOCUMENT TYPE	LEGISLATION	STATUTORY REQUIREMENT/BASIS FOR RETENTION	FOUNDATION & ACADEMY TRUST
COMPANY RECORDS			
Company Articles of Association, Rules / bylaws	Companies Act 2006 Charities Act 2011	Permanent	
Academy funding agreement and any supplemental agreements	Charities Act 2011	Permanent	
Trustee / director minutes of meetings and written resolutions	Companies Act 2006 Charities Act 2011	Recommended at least 10 years	Permanent – transfers to Archive
Members' meetings etc. Minutes / resolutions	Companies Act 2006 Charities Act 2011	Recommended at least 10 years	Permanent – transfers to Archive
Documents of clear historical / archival significance	Data Protection regulation	Permanent if relevant data protection regulation provisions are met. At the time of writing the Data Protection Bill contains relevant provisions but these are expected to change as the Bill goes through the parliamentary process. Legal advice should be obtained once the Data Protection Act 2018 is published.	
Contracts e.g. with suppliers or grant makers	Limitation Act 1980	Length of contract term plus 6 years	
Contracts executed as deeds	Limitation Act 1980	Length of contract term plus 12 years	
IP records and legal files re provision of service	Limitation Act 1980	Recommended: Life of service provision or IP plus 6 years	

TAX AND FINANCE			
Annual accounts and review (including transferred records on amalgamation)	Companies Act 2006 Charities Act 2011	Minimum 6 years Recommended: permanent record	

Tax and accounting records	Finance Act 1998 Taxes Management Act 1970	6 years from end of relevant tax year	
Information relevant for VAT purposes	Finance Act 1998 and HMRC Notice 700/21	Minimum 6 years from end of relevant period	
Banking records / receipts book/sales ledger	Companies Act 2006 Charities Act 2011	6 years from transaction	
EMPLOYEE / ADMINISTRATION			
Payroll / Employee / Income Tax and NI records: P45; P6; PIID; P60, etc.	Taxes Management Act 1970 / IT (PAYE) Regulations	6 years from end of current year	
Maternity pay	Statutory Maternity Pay Regulations	3 years after the end of the tax year	
Sick pay	Statutory Sick Pay (General) Regulations	3 years after the end of the tax year	
National Minimum wage records	National Minimum Wage Act	3 years after the end of the tax year	
Foreign national ID documents	Immigration (Restrictions on Employment) Order 2007 Independent School Standards Regulations	Minimum 2 years from end of employment	

HR files and training records	Limitation Act 1970 and Data Protection regulation	Maximum 6 years from end of employment	
Records re working time	Working Time Regulations 1998 as amended	2 years	
Job applications (CVs and related materials re unsuccessful applicants)	ICO Employment Practices Code (Recruitment & Selection) Disability Discrimination Act 1995 & Race Relations Act 1976	Recommended: 6-12 months from your notification of outcome of application	
Pre-employment / volunteer vetting	ICO Employment Practice Code Independent School Standards Regulations	6 months	

Disclosure & Barring Service checks	Single Central Record Requirements under • for maintained schools: Regulations 12(7) and 24(7) and Schedule 2 to the School Staffing (England) Regulations 2009 and the School Staffing (England) (Amendment) Regulations 2013 (applied to pupil referral units through the Education (Pupil Referral Units) (Application of Enactments) (England) Regulations 2007); • for independent schools, (including academies and free schools and alternative provision academies and free schools): Part 4 of the Schedule to the Education (Independent School Standards) Regulations 2014;	Record only satisfactory / unsatisfactory result and delete other information. If copy is kept, not to be retained beyond 6 months See further DfE statutory Guidance ' Working Together to safeguard children' https://www.gov.uk/government/publications/working-together-to-safeguard-children--2	
Volunteer records		Undertake assessment to decide on retention period taking account of risk (e.g. safeguarding re work with children)	
Allegations of a child protection nature made against a member of staff (including unfounded allegations)	Employment Practices Code: Supplementary Guidance (Information Commissioner's Office)	Retain until the normal retirement age for the member of staff or for 10 years (whichever is the longer)	

INSURANCE			
Employer's Liability Insurance	Employers' Liability (Compulsory Insurance Regulation) 1998	40 years	
Policies	Commercial	3 years after lapse	
Claims correspondence	Commercial	3 years after settlement	
HEALTH & SAFETY / MEDICAL			
General records	Limitation Act 1970	Minimum 3 years	
Records re work with hazardous substances	Control of Hazardous Substances to Health Regulations 2002	Up to 40 years. Recommend: Permanent	
Accident books / records and reports	Reporting of Injuries Diseases and Dangerous Occurrences Regulations 1995	3 years after last entry or end of investigation	
Medical Scheme documentation	Commercial	Permanent unless personal data is included	
PREMISES / PROPERTY			
Original title deeds		Permanent / to disposal of property	
Leases	Limitation Act 1980	12 years after lease has expired	
Building records, plans, consents and certification and warranties etc	Limitations Act 1980	6 years after disposal or permanent if of historical / archival interest. Carry out review re: longer retention, e.g. if possible actions against contractors	

PENSION RECORDS			
Records about employees and workers	For all categories see: Detailed Guidance for Employers: (April 2017) pensions regulator.gov.uk		
Trustees' Minutes and annual accounts			
Policies including investment policies			
Records re the Scheme			
Records re active members and opt in / opt out			
Trust Deed / Rules and HMRC approvals			

PUPILS			
Educational Record	Pupil information Regulations 2005 (maintained schools only) Same approach applied in academy context. Data Protection regulation	25 years from date of birth if this is the final school of the child but the pupil file should follow the pupil, so it is likely to be difficult to justify the need for retention once the file has been passed to the pupil's new school	

Child Protection and Safeguarding information	"Keeping children safe in education Statutory guidance for schools and colleges 2021 "; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children February 2017" Government guidance: Data protection: toolkit for schools (see page 31).	Until the child is 25 years of age or older if required. 'Long term, until the child is 25 years of age or older, for instances where detailed information about activities in school may form an important part of safeguarding for that individual'.	The information should not be kept any longer than is necessary. In some rare circumstances, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so

Annual parents' meetings papers	Common Practice	Retain for 6 years	
Successful school admissions applications	Common Practice	Retain for 1 year	
Unsuccessful school admission applications (where no appeal is made)	School Admissions Appeals Code 2012	Retain for 1 year	

Unsuccessful school admission applications (where an appeal is made)	School Admissions Appeals Code 2012	Retain for 1 year from resolution of case	
Proofs of address supplied by parents as part of the admissions process	Common practice	Retain for 1 year from date of admission	
Attendance registers	Common practice	Retain for 3 years	
SPECIAL EDUCATIONAL NEEDS			
SEN files	Limitation Act 1980 and Special Educational Needs and Disability Act 2001	Usually 25 years from date of birth of the pupil. If kept longer show good justification.	
Education Health and Care Plans	Special Educational Needs and Disability Regulations 2014 Children and families Act 2014, part 3	25 years from date of birth of the pupil	
Statements of Special Educational Needs (now historic)	Originally under Special Educational Needs and Disability Regulations 2001	25 years from date of birth of pupil unless passed to new school (usually on the pupil's file)	
Attendance registers	Pupil Registration Regulations 2006 Regulation 14	3 years from when the register entry was made if made in paper registers	

		For computerised registers retain until 3 years after the end of the school year during which the entry was made. This applies to every back up copy. The difference in retention periods as between manual and computerised registers has probably come about in error but this is what the Regulations say.	
Other items e.g. curriculum related, photographs, video recordings	Case by case basis	Look at why you are processing this and how long you need it for. Make sure you have a good justification for keeping it as long as you do. Set out the items and the justification.	
PARENTS			
Parent details	Pupil Registration Regulations 2006 For basic name and contact details. Otherwise usually operational in accordance with the statutory functions of the school	Usually, for the duration that the parent has a pupil at the school. Otherwise subject to case by case justification.	
ALUMNI / ALUMNAE			
Policy Documents	Common practice	Retain while policy is used operationally.	Move to archive
Complaints files	Common practice	Retain for 6 years	Destroy after 6 years if noncontentious

Annual reports required by central government	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	Retain for 10 years	
KING EDWARD'S CONSORTIUM SPECIFIC			
UCAS application form (successful)	Limitation Act 1980 c.58	End of student relationship + 6 years maximum	KEC retain on HR file for duration of course and for 2 years after completion of course
UCAS application form (unsuccessful)	JISC	Retain for 1 year	
KEC additional information form (successful)	Limitation Act 1980 c.58	End of student relationship + 6 years maximum	KEC retain on HR file for duration of course and for 2 years after completion of course
KEC additional information form (unsuccessful)	JISC	Retain for 1 year	
Additional references form	Limitation Act 1980 c.58	End of student relationship + 6 years maximum	KEC retain on HR file for duration of course and for 2 years after completion of course
Academic qualifications (copy certificates)	Limitation Act 1980 c.58	Retention variable for different types of personal data up to a maximum of: End of registered student relationship +6 years	KEC retain for 2 years after completion of course
KEC interview notes and entrance tests (successful)		Retain on HR file for duration of course and for 2 years after completion of course	
KEC interview notes and entrance tests (unsuccessful)		Retain for 1 year	
School-based interview notes (salaried trainees only)	Limitation Act 1980 c.58	End of student relationship + 6 years maximum	KEC retain on HR file for duration of course and for 2 years after completion of course

Safer recruitment checks confirmation letters to schools	Limitation Act 1980 c.58	Retention variable for different types of personal data up to a maximum of: End of registered student relationship +6 years	KEC retain for 2 years after completion of course
Disclosure & Barring Service checks (Strictly Education)	Keeping children safe in education 2018 (Statutory Guidance from Dept. of Education) Sections 73, 74	Retain on HR file for duration of course and for 2 years after completion of course	

Fit to Teach medical		Retain on HR file for duration of course and for 2 years after completion of course	
Right to work check - evidence	An employer's guide to right to work checks (Home Office January 2019)	Retain on HR file for duration of course and for 2 years after completion of course	
KEC Contract for fee-paying trainees	Limitation Act 1980	End of the contract + 6 years	
Code of Professional Conduct and Fitness to Practice		Retain on HR file for duration of course and for 2 years after completion of course	
SKE certificate/ confirmation		Retain on HR file for duration of course and for 2 years after completion of course	
Self-certification absence form		Retain on HR file for duration of course and for 2 years after completion of course	
Correspondence		Retain on HR file for duration of course and for 2 years after completion of course	
References from KEC for NQT posts		End of student relationship + 6 years maximum	
Training records		Retain on HR file for duration of course and for 2 years after completion of course	

Final report		End of student relationship + 6 years maximum	
Student database entry	Limitation Act 1980 c.58	Retention variable for different types of personal data up to a maximum of: End of registered student relationship +6 years	KEC retain for 2 years after completion of course
Handling of formal complaints made by individual students	Limitation Act 1980 c.58	Last action + 6 years	
Handling of complaints made by individual students where the formal complaints procedure is not initiated	JISC	Last action + 3 years	

OTHER INFORMATION			
Minutes of management team	Common practice	Retain for 5 years	
Development plans	Common practice	Retain for 6 years	
Other information	various	Please consult the IRMS toolkit for schools which is here: http://irms.org.uk/page/SchoolsToolkit	

F.1 When a document is at the end of its retention period it should be either destroyed via confidential waste or deleted electronically with IT support.

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 is not used for marketing.

END.