Contents:

Appendices:

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

a) The General Data Protection Regulation (GDPR);
b) The Freedom of Information Act 2000;
c) The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016);
d) The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004;
e) The School Standards and Framework Act 1998.

1.2. This policy will also have regard to the following guidance:

a) Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
b) Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

2. Applicable data

2.1. For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data.

2.2. Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Principles

3.1. In accordance with the requirements outlined in the GDPR, personal data will be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
g) The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1. The Archbishop Lanfranc Academy will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

5. Data protection officer (DPO)

5.1. A DPO will be appointed in order to inform and advise the Academy and its employees about their obligations to comply with the GDPR and other data protection laws.

5.2. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the GDPR, data will be lawfully processed under the following conditions:

a) The consent of the data subject has been obtained;
b) Appendix A. The Academy Fair Processing Notice

6.3. Sensitive data will only be processed under the following conditions:

a) Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law;
b) Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent;
c) Processing relates to personal data manifestly made public by the data subject;
d) Processing is necessary for: — carrying out obligations under employment, social security or social protection law, or a collective agreement. — Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent. — The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity. — Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards. — The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional. — Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices. — Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

7. Consent

7.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre ticked boxes.

7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given.

8. The right to be informed

8.1. The privacy notice supplied to individuals in regard to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

9. The right of access

9.1. Individuals have the right to obtain confirmation that their data is being processed.

9.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

9.3. The Academy will verify the identity of the person making the request before any information is supplied.

9.4. A copy of the information will be supplied to the individual free of charge; however, the Academy may impose a 'reasonable fee' to comply with requests for further copies of the same information.

9.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

9.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

9.7. All fees will be based on the administrative cost of providing the information.

9.8. All requests will be responded to without delay and at the latest, within one month of receipt.

9.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.10. Where a request is manifestly unfounded or excessive, the Academy holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.11. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

10. The right to rectification

10.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

10.2. Where the personal data in question has been disclosed to third parties, the Academy will inform them of the rectification where possible.

10.3. Where appropriate, the Academy will inform the individual about the third parties that the data has been disclosed to.

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5. Where no action is being taken in response to a request for rectification, the Academy will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to be forgotten

11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. Individuals have the right to erasure in the following circumstances:

a) Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
b) When the individual withdraws their consent
c) When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
d) The personal data was unlawfully processed
e) The personal data is required to be erased in order to comply with a legal obligation
f) The personal data is processed in relation to the offer of information society services to a child

11.3. The Academy has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

a) To exercise the right of freedom of expression and information
b) To comply with a legal obligation for the performance of a public interest task or exercise of official authority
c) For public health purposes in the public interest
d) For archiving purposes in the public interest, scientific research, historical research or statistical purposes
e) The exercise or defence of legal claims

11.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

11.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11.6. Where personal data has been made public within an online environment, the Academy will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. The right to restrict processing

12.1. Individuals have the right to block or suppress the Academy's processing of personal data.

12.2. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

12.3. The Academy will restrict the processing of personal data in the following circumstances:

a) Where an individual contests the accuracy of the personal data, processing will be restricted until the Academy has verified the accuracy of the data
b) Where an individual has objected to the processing and the Academy is considering whether their legitimate grounds override those of the individual
c) Where processing is unlawful and the individual opposes erasure and requests restriction instead
d) Where the Academy no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

12.4 If the personal data in question has been disclosed to third parties, the Academy will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

13. The right to data portability

13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

13.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

13.3. The right to data portability only applies in the following cases:

a) To personal data that an individual has provided to a controller
b) Where the processing is based on the individual's consent or for the performance of a contract
c) When processing is carried out by automated means

13.4. Personal data will be provided in a structured, commonly used and machine-readable form.

13.5. The Academy will provide the information free of charge.

13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7. The Academy is not required to adopt or maintain processing systems which are technically compatible with other organisations.

13.8. In the event that the personal data concerns more than one individual, the Academy will consider whether providing the information would prejudice the rights of any other individual.

13.9. The Academy will respond to any requests for portability within one month.

13.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

13.11. Where no action is being taken in response to a request, the Academy will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. The right to object

14.1. The Academy will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2. Individuals have the right to object to the following:

a) Processing based on legitimate interests or the performance of a task in the public interest
b) Direct marketing
c) Processing for purposes of scientific or historical research and statistics.

14.3. Where personal data is processed for the performance of a legal task or legitimate interests:

a) An individual's grounds for objecting must relate to his or her particular situation;
b) The Academy will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Academy can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

14.4. Where personal data is processed for direct marketing purposes:

a) The Academy will stop processing personal data for direct marketing purposes as soon as an objection is received;
b) The Academy cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

14.5. Where personal data is processed for research purposes:

a) The individual must have grounds relating to their particular situation in order to exercise their right to object;
b) Where the processing of personal data is necessary for the performance of a public interest task, the Academy is not required to comply with an objection to the processing of the data.

14.5. Where the processing activity is outlined above, but is carried out online, the Academy will offer a method for individuals to object online.

15. Data breaches /breach management

15.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

15.2. The DPO will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

15.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

15.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Academy becoming aware of it.

15.5. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

15.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

15.7. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

15.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

16. Data security

16.1. Confidential paper records will be kept in a locked filing cabinet or drawer with restricted access.

16.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

16.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

16.4. Any portable memory device (such as a USB or external hard drive) used for the storage of data will be encrypted and password protected. Non-encrypted devices will not be compatible with Academy computer systems.

16.5. All electronic devices are password-protected to protect the information on the device in case of theft.

16.6. Where possible, the Academy enables electronic devices to allow the remote blocking or deletion of data in case of theft.

16.7. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

16.10 Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Academy’s premises accepts full responsibility for the security of the data.

16.8. Before sharing data, all staff members will ensure;

a) They are allowed to share it;
b) That adequate security is in place to protect it.

16.9. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Academy containing sensitive information are supervised at all times.

16.10. The Archbishop Lanfranc Academy takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

17. Publication of information

17.1. The Archbishop Lanfranc Academy publishes on its website information that will be made routinely available, including:

a) Policies and procedures
b) Annual reports
c) Financial information

18. CCTV and photography

18.1. The Academy understands that recording images of identifiable individuals counts as processing personal information and therefore this is done in line with data protection principles.

18.2. The Academy notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards.

18.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

18.4 All CCTV footage will be retained for up to ten days for security purposes; the DPO is responsible for keeping the records secure and allowing access. CCTV footage captured in relation to wrongdoing on the site will be kept for as long as necessary as to be of use to the Academy investigating officer or law enforcement agencies.

18.4. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

19. Data retention

19.1. Data will not be kept for longer than is necessary (See Appendix C- HR Records and Management protocol and Appendix D -Retention Register)

19.2. Unrequired data will be deleted as soon as practicable.

19.3. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

19.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

20. DBS data

20.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

20.2. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

21. Policy review

Effective from: 1st September 2021
Approved by Governing Body:
Review date: May 2023

Appendix A - **Privacy Notice (How we use pupil information)**

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information
- SEN information
- Behaviour information, including information regarding exclusions
- CCTV footage

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care and safeguarding
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use pupil information under Article 6.1e) of GDPR, and Article 9.2b) in the instance of special categories of information.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data for 5 years after a pupil has left the school.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- school nurse, and other relevant health professionals

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.
We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services- Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

Pupils aged 16+

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

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

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

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

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

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact **Mr R Ellis.**

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact
If you would like to discuss anything in this privacy notice, please contact: **Mr R Ellis**

Appendix B- Privacy Notice (How we use school workforce information)

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, employee or teacher number, national insurance number)
- addresses
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- payroll number

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid

The lawful basis on which we process this information

We process this information under Article 6.1e) of GDPR, and Article 9.2b) in the instance of special categories of information.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We hold school workforce data for 3 years after the term of employment

Who we share this information with

We routinely share this information with:

- our local authority
- the Department for Education (DfE)

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority
We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our pupils with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Academys) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

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

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

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

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

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

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

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

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

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the Data Protection Officer.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact: **Mr R Ellis**

Appendix C

HR Records Management Protocol

1. Introduction

1.1 It is important to maintain effective systems for storing HR data, to ensure compliance with the myriad of relevant legislation and to support both sound HR administration and broader HR strategy.

1.2 Records may be hard or soft copy documents (paper files, databases, spread sheets, word processing packages, etc.) and may consist of letters, memos, emails, reports, minutes, personal records or tables of information. They may also be held in the form of tape recordings, videos, cds, microfiche or more advanced media.

1.3 The Data Protection Act 1998 applies to most HR records. The Act stipulates that data must not be kept any longer than is necessary for a particular purpose. Employees have the right to access their own records and we are obliged to ensure that data kept is accurate. Before releasing any of that data to a third party, we must seek the permission of the individual concerned.

1.4 There is a large and complex regulatory regime which impacts on the retention of records. Our protocol on each of these areas is as follows:

1.5 **Table 1 – description of records**

Record type	Retention Period	Reason
Recruitment: Advertisement, job description (JD), application form, references , medical clearance, DBS record number, ID, contract, required qualifications to work, permission to work in the UK, etc. for unsuccessful candidates: for successful candidates :	 End of the Academy term in which the application process has occurred Duration of employment plus 6 years	Limitation Act 1980, for audit purposes and to allow for time limits for bringing claims
Employment : Induction checklist, offer letter, probation report, pay, enhancements, market supplements, personal info (dob, address, etc.), internal transfers, secondments etc., OH referrals, absence, lateness, complaints , capability issues, recoverable benefits such as car loan, travel loan, relocation expenses, etc., parental leave agreement, resignation letter, marital status, mortgage/accommodation references, training record, name changes, home address changes, letter to DBS reporting unsuitability to work with children/vulnerable people, management advice, file notes, use of internet/ email acceptance, termination of employment details. requests for references and their responses, dismissal	6 years after leaving – permanent for staff working with children or vulnerable people.	Limitation Act 1980, for audit purposes and to allow for time limits for bringing claims

information, job description of last post held, signed AUP Policy, signed Policies and Procedures policy, signed Disqualification and Disqualification by association, staff TUPE transferred, secondment agreement, appraisals, emergency contact, identification and recovery of monies owed to the Academy, selection for redundancy		
Fixed term workers Record of fixed term review meeting Outcome letters End of fixed term contract Letter making fixed term a permanent position	 1 year 1 year Termination of employment + 6 years Termination of employment + 6 years	Limitation Act 1980
Legal cases ET investigations, papers and case files, compliance with statutory requests from HMRC, Benefits Agency, other authorities/agencies.	Closure of case + 6 years, regardless of outcome	Limitation Act 1980
Equalities Monitoring Personal profile/ monitoring information	6 years after leaving	Equality Act 2010
Medical / Health and safety records Accident/injury reports, RIDDOR form, risk assessments, industrial injury form, ill health retirement letter	40 years from date of last entry	COSHH, RIDDOR CAW, CLW, IRR Regs
Maternity MATB1 form , application for maternity leave, parental leave, paternity leave, adoption leave	3 years after the end of the tax year the maternity leave ends – remove after 6 years along with rest of file	SMP Regs
Sickness Paid and unpaid sickness absence and pay record, doctors' certificates, self-certificates and fit notes	3 years after the end of the tax year to which sickness records relate (certificates and fit notes held by manager, not HR)	SSPay Regs
National minimum wage records Pay history , termination pay, redundancy pay, notice pay, outstanding holiday pay	3 years after the end of the period the records cover	NMWA 1998
Working time records Opt out agreement, flexible working arrangement, hours worked	2 years from date they were made	WT Regs
Pay Inc.	Termination + 6 years	Taxes Management Act 1970
Disciplinary documentation: a) Investigation and hearing records related to protection of children and vulnerable people b) Investigation records relating to bullying and Harassment c) Records where investigation concludes no further action necessary	 15 years after case closed 6 years after case closed 6 months after case closed	Limitation Act 1980

d)	Record where charges are dismissed at the hearing stage	6 months after case closed	
e)	Records where matter reaches the hearing stage and at least one allegation is upheld	2 years after case closed	
f)	Warning and /or dismissal letters relating to protection of children and vulnerable people	15 years after end of employment	
g)	Other warning or dismissal letters	6 years after warning expires unless concern continues , in which case until case is closed	

2. Access, Storage, Format and Destruction Methods

2.1 Subject to certain exceptions, employees have the right to access their records and we are obliged to ensure that data is accurate. Before releasing such data to a third party, we must seek permission from the individual concerned.

2.2 If employment contracts, accident records or other HR records are needed for the purposes of legal action, copies of original documents must be made available if possible (in accordance with Table 1 above) , or we have to be able to explain what happened to them, backed up by a 'statement of truth'.

2.3 When we no longer need to keep certain data, its destruction must take place securely (shredding, for example).

2.4 Further special provisions may arise which affect the retention of or access to data, e.g.:

a) In the context of criminal law, the Anti-Terrorism, Crime and Security Act 2001 provides a lengthy code of practice for voluntary retention of communications data;

b) To provide security services with a reliable log of phone calls, telecoms companies must keep telephone call logs for a year. Internet service providers must retain comms data for a year;

c) In the field of immigration, the UK Borders Act 2007 and the Immigration, Asylum and Nationality Act 2006 may enable access to HR records in certain circumstances.

Appendix D- Guidance for Staff

What staff should do:

DO get the permission of your line manager to take any confidential information home.
DO ensure that when posting/emailing information that only the specific content required by the recipient is sent.
DO use pseudonyms and anonymise personal data where possible.
DO ensure that access to SIMS (or equivalent) is restricted to appropriate staff only, that leavers are removed in a timely manner and that generic user names such as 'Sysman' are disabled.
DO ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post, the envelope should clearly state 'Private – Contents for Addressee only'.
DO avoid taking paper documents out of the office, wherever possible.
DO shred or burn documents including people's names as soon as they are no longer needed. (Guidance for retention periods can be found at https://irms.site-ym.com/page/SchoolsToolkit).

If you must use paper…what staff should do:

DO ensure that all paper based information that is taken off premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.
DO ensure that any confidential documents that are taken to your home are stored in a locked drawer.
DO ensure that paper based information and laptops are kept safe and close to hand when taken off premises; never leave them unattended. Particular care should be taken in public places (e.g. reading of documentation on public transport).
DO ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.
DO return the paper based information to the academy as soon as possible and file or dispose of it securely.
DO report any loss of paper based information or portable computer devices to your line manager immediately.

Electronic Communication - What staff should do:

DO use secure, portable computing devices such as encrypted laptops and encrypted USB memory sticks when transporting information from the academy, working remotely or from home.
DO ensure that any information on USB memory sticks is securely deleted off the device, or saved on an academy shared drive.
DO ensure that all e-mail addresses are checked to ensure safe dispatch of information. Use bcc (blind copy), rather than cc, to avoid inadvertently sharing confidential e-mail addresses).

What staff must not do:

DO NOT take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.
DO NOT unnecessarily copy other parties into e-mail correspondence.
DO NOT e-mail documents to your own personal computer.
DO NOT store work related documents on your home computer.
DO NOT leave personal information unclaimed on any printer or fax machine.
DO NOT leave personal information on your desk overnight, or if you are away from your desk in meetings.
DO NOT display personal information on whiteboards.
DO NOT leave computers unlocked.
DO NOT allow pupils to use computers with your log-in.