HEARTWOOD
LEARNING TRUST

DATA PROTECTION (UK GDPR) POLICY

THIS POLICY APPLIES TO THE HEARTWOOD LEARNING TRUST BOARD, THE CENTRAL TEAM, AND ALL TRUST SCHOOLS/ACADEMIES

Document Management	
Updated Policy Approved	March 2026
Next Review Date	March 2027
Version	2.1
Approving Committee	Trust Board

Contents

Policy Updates 2
Introduction 3
Statement of Intent 3
1. Legal Framework 4
2. Roles and Responsibilities 4
3. Applicable Data 6
4. Accountability 7
5. Data Protection Officer (DPO) 8
6. Lawful Processing 9
7. Consent 11
8. The Right to be Informed 11
9. The Right of Access 12
10. The Right to Rectification 13
11. The Right to Erasure 14
12. The Right to Restrict Processing 15
13. The Right to Data Portability 15
14. The Right to Object 16
15. Automated Decision Making and Profiling 17
16. Data Protection by Design and Default 18
17. Data Protection Impact Assessments (DPIAs) 18
18. Data Breaches 19
19. Data Security 20
20. Safeguarding 21
21. Publication of Information 21
22. CCTV and Photography 22
23. Cloud Computing 23
24. Data Retention 24
25. DBS Data 24
26. Monitoring and Review 24
Appendix A - Data Retention Schedule 25
- Pupil records and other pupil-related information 26
- Employee Records 34
- Governance Records 37
- Leadership and Management Records 42
- Health and Safety Records 44
- Retention of Financial Records 47
- Administrative Records 53

Appendix B - Nominated GDPR Representatives 55

Policy Updates

Date	Page	Policy Updates
February 2026	Whole policy	References to Compliance Officer changed to Executive Support Manager (under Line Management)
February 2026	3	Introduction added in line with other Trust Policies
February 2026	3	Statement of Intent wording updated
February 2026	4	1 - Legal Framework updated to reflect current applicable legislation, guidance and policies
February 2026	4	2 - Roles and Responsibilities section added
February 2026	7	3.7 - Point added regarding standardised data collection and consent forms
February 2026	10	6.5 - Added reference to GDPR privacy notices
February 2026	12	9 - Right of Access updated to reflect the need to verify ID and how records are shared
February 2026	17	15 - New section added re: Complaints
February 2026	20	19 - Minor wording updated for clarification
February 2026	22	21.4 - Added point re: harm threshold test
February 2026	22	23.3 - Updated to reflect access to CCTV monitoring being restricted
February 2026	24	26.3 - Monitoring and Review updated to reflect where the policy can be accessed
February 2026	25	Data Retention Schedule updated

Introduction

Heartwood Learning Trust is an inclusive and collaborative Church of England multi-academy trust serving church, community and alternative provision schools. This policy is guided by our Christian ethos and the visions of our Trust and its schools/academies. We share a clear vision – to create schools where children and young people thrive, as we help them prepare to live life in all its fullness (John 10:10).

For us, a place to thrive means much more than a place simply to be comfortable. Instead, our aim is to develop schools and an educational offer which enable each pupil to flourish academically, practically, emotionally, socially and spiritually.

Statement of Intent

Heartwood Learning Trust is required to keep and process certain information (including personal data) about our employees, pupils, parents/carers, volunteers and external contractors in accordance with our legal obligations under data protection legislation.

The Trust may be required to share personal data about its employees or pupils with external organisations, such as the Local Authority (LA), Department for Education (DfE), other schools/academies and third-party support agencies such as Children's Services.

This policy is in place to ensure all employees, Trustees and Governors are aware of their responsibilities regarding data protection and outlines how the Trust complies with the core principles of the **UK GDPR**.

Organisational methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

The Trust has appointed a **Data Protection Officer (DPO)** in order to comply with the requirements placed on schools/academies and ensure we remain compliant with applicable data protection legislation. The **DPO** will be the central point of contact for all Data Subjects in relation to matters of data protection.

1. Legal Framework

1.1. This policy has due regard to all relevant **legislation** and **statutory guidance** including, but not limited to, the following:

- Protection of Freedoms Act 2012
- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- DfE 'Keeping children safe in education (KCSiE)' (as amended)

1.2. This policy operates in conjunction with the following **guidelines**:

- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE (2023) 'Data protection in schools'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2018) 'Data protection: a toolkit for schools'
- ESFA (2022) 'Record keeping and retention information for academies and academy trusts'
- Information Records Management Society (IRMS) (2019) 'Information Management Toolkit for Schools'
- IRMS (2019) 'Academies Toolkit'

1.3. This policy operates in conjunction with the following **Trust** policies:

- Photography and Videos at School Policy
- Freedom of Information Policy and Model Publication Scheme
- CCTV Policy
- Safeguarding and Child Protection Policy
- Subject Access Request (SAR) Policy and Procedures
- Data Breach Policy and Procedures
- Special Category Data Policy
- Data Asset Register

2. Roles and Responsibilities

2.1. The **Trust Board** is responsible for:

- Reviewing and approval of this policy in line with the Trust's policy review schedule
- Monitoring the Trust's compliance with the **UK GDPR** as **Data Controller**

2.2. The **Data Protection Officer (DPO)** is responsible for:

- Monitoring the overall implementation and effectiveness of this policy across the Trust
- Maintaining good levels of knowledge regarding data protection law, particularly in relation to schools/academies

- Overseeing the Trust's compliance with the **UK GDPR**
- Overseeing the Trust's internal data protection activities and calculating and evaluating the associated risks
- Having due regard to the nature, scope, context, and purposes of all data processing across the Trust
- Ensuring adequate provisions are in place to protect the personal rights and freedoms of all Data Subjects whose personal data is being processed by the Trust
- Coordinating a proactive and preventative approach to data protection
- Reviewing and responding to any complaints regarding the Trust's processing of personal data
- Reviewing half-termly reports on GDPR across the Trust
- Reporting to the **Trust Board** on the Trust's compliance with the **UK GDPR**, as required
- Reporting any serious breaches of personal data to the **Information Commissioner's Office (ICO)**, as required on behalf of the Trust
- Reviewing and approval of **Data Protection Impact Assessments (DPIAs)** across the Trust
- Conducting internal audits, as required
- Ensuring employees are aware of their obligations to comply with the **UK GDPR**
- Providing advice and guidance on data protection relating enquiries, as required
- Promoting a culture of data privacy awareness across the Trust

2.3. The **Executive Support Manager (ESM)** is responsible for:

- Ensuring this policy is updated every two years, or earlier if there are any significant changes in applicable data protection legislation
- Managing the Trust's internal data protection activities on a day-to-day basis
- Being the main point of contact for employees' GDPR related queries, escalating any serious concerns or items for approval to the **DPO**
- Acting as the first point of contact for the **ICO**, as required
- Ensuring that **DPIAs** are reviewed and monitored to ensure consistency and accuracy of information
- Ensuring that **DPIAs** are completed on behalf of the Trust, as required, and are submitted to the **DPO** for final approval
- Maintaining accurate records of **DPIAs** and the **Register of Processing Activities (ROPA)** Trust wide
- Ensuring that approved **DPIAs** are published and notifying employees of permissions to utilise the applicable software/applications
- Completing data protection refresher training as required
- Ensuring the nominated **GDPR Representatives** have received suitable training for their role
- Promoting a culture of data privacy awareness amongst the nominated **GDPR Representatives**
- Assisting the **DPO** to implement a proactive and preventative approach to data protection across the Trust
- Having due regard to the nature, scope, context, and purposes of all data processing across the Trust
- Reviewing and conducting internal audits, as appropriate and in conjunction with the **DPO**
- Carrying out ad hoc reviews of data practices to ensure nominated **GDPR Representatives** understand and are acting in accordance with relevant data protection legislation

2.4. The nominated **GDPR Representatives** are responsible for:

- Representing the **DPO** at a local level for their individual school/academy and being the main point of contact for employees' GDPR related queries
- Escalating any GDPR queries to the **ESM**, as appropriate
- Completing data protection training, as requested by the **ESM**
- Carrying out ad hoc reviews of data practices to ensure employees at the school/academy understand and are acting in accordance with the Trust's **Data Protection (UK GDPR) Policy**
- Promoting a culture of data privacy awareness across the school/academy

2.5. The Trust's **External IT Provider** is responsible for:

- Ensuring the Trust's IT systems are secure and compliant with the **UK GDPR**
- Reporting to the **DPO** any issues or concerns regarding IT and personal data

2.6. **Employees** are responsible for:

- Reading and understanding this policy, seeking clarification from the nominated **GDPR Representative** or **ESM**, as required
- Adhering to the provisions outlined in this policy to comply with the requirements of the **UK GDPR**
- Reporting any concerns in relation to data protection to, and seeking guidance from the nominated **GDPR Representative** or **ESM**, as required

3. Applicable Data

3.1. 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, e.g. an IP address. The **UK 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 and pseudonymised data, e.g. key-coded.

3.2. **'**Sensitive personal data' is referred to in the **UK GDPR** as 'special categories of personal data', and is defined as:

- Genetic data
- Biometric data
- Data concerning health
- Data concerning a person's sex life
- Data concerning a person's sexual orientation
- Personal data which reveals:
    - Racial or ethnic origin
    - Political opinions
    - Religious or philosophical beliefs
    - Trade union membership
    - Principles

3.3. 'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools/academies are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law

3.4. The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

3.5. In accordance with the requirements outlined in the **UK GDPR**, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- 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
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 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
- 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 **UK GDPR** in order to safeguard the rights and freedoms of individuals
- 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

3.6. The **UK GDPR** also requires that "the controller shall be responsible for, and able to demonstrate, compliance with" the above principles.

3.7. The Trust ensures that schools/academies utilise a standardised template form for data collection and parental consent, in line with the Department for Education (DfE)'s pupil data requirements. Upon admission to the school/academy, parents/carers will be required to complete a **Data Collection Form** to provide essential information regarding their child(ren). The Trust will ensure that alternative arrangements are in place, such as translated data collection forms, for pupils of families where English is not their first language. The school/academy will also communicate with parents/carers on an annual basis each September to ensure that information held on the school/academy's management information system (MIS) remains accurate and up to date; pupil **Data Collection Forms** may be redistributed should any changes be required.

4. Accountability

4.1. The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the **UK GDPR**, and will provide comprehensive, clear and transparent privacy policies.

4.2. The Trust will be able to demonstrate how data is processed across the Trust, and will ensure each individual school/academy is adhering to the same procedure and that this is being implemented and

enforced in line with the wider Trust policies.

4.3. Additional internal records of the school/academy's processing activities will be maintained and kept up-to-date.

4.4. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4.5. The Trust will also document other aspects of compliance with the **UK GDPR** and **Data Protection Act** where this is deemed appropriate in certain circumstances by the **DPO**, including the following:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- **Data Protection Impact Assessments (DPIAs)**
- Records of personal data breaches

4.6. The Trust and the individual schools/academies will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Minimising the processing of personal data
- Pseudonymising personal data as soon as possible
- Ensuring transparency in respect of the functions and processing of personal data
- Allowing individuals to monitor processing
- Continuously creating and improving security features

4.7. **DPIAs** will be used to identify and reduce data protection risks, where appropriate.

5. Data Protection Officer (DPO)

5.1. Our Trust has an appointed **DPO** in order to comply with the requirements placed on schools and academies. The **DPO** will be the central point of contact for all data subjects and others in relation to matters of data protection. Each school/academy within the Trust has a nominated **GDPR Representative** (see **Appendix B**).

5.2. A **DPO** will be appointed in order to:

- Inform and advise the Trust and the individual schools/academies and its employees about their obligations to comply with the **UK GDPR** and other data protection laws.
- Monitor the Trust and the individual school/academy's compliance with the **UK GDPR** and other laws, including managing internal data protection activities, advising on **DPIAs**, conducting internal audits, and providing the required training to staff members.

- Cooperate with the **ICO** and act as the first point of contact for the **ICO** and for individuals whose data is being processed.

5.3. The **DPO** is responsible for:

- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the school/academy's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the school community.
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws.

5.4. The Trust employs the services of an external IT provider. The external IT provider reports to the **Chief Operating Officer (COO)** (who is also the **DPO**).

5.5. The individual appointed as **DPO** will have professional experience and be highly knowledgeable about data protection law, particularly that in relation to schools. 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.

5.6. The **DPO** will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the **DPO** to enable them to meet their **UK GDPR** obligations.

5.7. The **DPO** will report to the highest level of management at the Trust, which is the **Trust Board**. Staff will ensure that they involve the **DPO** in all data protection matters closely and in a timely manner.

6. Lawful Processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed. Under the **UK GDPR**, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual, or because they have asked the Trust/school/academy to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the school/academy in the performance of its tasks

6.2. The school/academy will only process personal data without consent where any of the above purposes

cannot reasonably be achieved by other, less intrusive means or by processing less data.

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

- Explicit consent of the data subject
- 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
- Processing relates to personal data manifestly made public by the data subject. 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 with a basis in 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 with a basis in law
    - 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 a basis in law

6.4. When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

6.5. The Trust will ensure that it has **Privacy Notices** in place which clearly outline the reasons why we need to collect personal data, how long data will be retained for and who this may be shared with. **Privacy Notices** will be clear and accessible for Data Subjects to understand - and stakeholders will be updated where there are any significant changes in how the Trust processes personal data.

6.6. For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed
- Why the personal data is being processed
- What the lawful basis is for that processing
- Whether the personal data will be shared, and if so, with whom
- The existence of the data subject's rights in relation to the processing of that personal data
- The right of the data subject to raise a complaint with the **ICO** in relation to any processing

6.7. The Trust provides privacy notices for the following groups, which outline the information above that is specific to them:

- Pupils
- Parents/carers

- Employees
- Members, Trustees and Governors

6.8. There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the **DPO** will be consulted and a decision made only after seeking further clarification.

6.9. Where the school/academy relies on:

- 'Performance of contract' to process a child's data, the school/academy considers the child's competence to understand what they are agreeing to, and to enter into a contract
- 'Legitimate interests' to process a child's data, the school/academy takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place
- Consent to process a child's data, the school/academy ensures that the school/academy does not exploit any imbalance of power in the relationship between the school/academy and the child

7. Consent

7.1. Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

7.2. Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

7.3. The school/academy ensures that consent mechanisms meet the standards of the **UK GDPR**. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent accepted under the **Data Protection Act (DPA)** will be reviewed to ensure it meets the standards of the **UK GDPR**; however, acceptable consent obtained under the **DPA** will not be reobtained.

7.4. When pupils and employees join the school/academy, the employee or pupil (or, where appropriate, pupil's parent/carer) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to complete a consent form.

7.5. Where the school/academy opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school/academy obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school/academy on a case-by-case basis, taking into account the requirements outlined above.

8. The Right to be Informed

8.1. Adults and children have the same right to be informed about how the school/academy uses their data.

The **Privacy Notices** supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

- **Privacy Notices** for Pupils, Parents/Carers, Members, Trustees and Governors are available on each school/academy website. They can also be accessed via the Trust website here.

8.2. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within or alongside the privacy notice:

- The identity and contact details of the controller, the controller's representative, where applicable, and the **DPO**
- The purpose of, and the lawful basis for, processing the data
- The legitimate interests of the controller or third party
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place
- The retention period of criteria used to determine the retention period
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time
    - Lodge a complaint with a supervisory authority
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences

8.3. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided - this information will be supplied at the time the data is obtained.

8.4. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school/academy holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided - this information will be supplied:

- Within one month of having obtained the data
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed
- If the data are used to communicate with the individual, at the latest, when the first communication takes place

9. The Right of Access

9.1. Please refer to the Trust's **Subject Access Request (SAR) Policy** and **Subject Access Request (SAR) Procedures** for more information regarding the data subject's right of access.

9.2. Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed, and 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. The Trust will verify the identity of the person making the request before any information is disclosed. When the Trust receives a SAR, the requestor will be asked to provide reasonable evidence in order for the Trust to confirm their identity.

9.3. A copy of the information will be supplied to the individual free of charge; however, the school/academy may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are

manifestly unfounded or excessive or if an individual requests further copies of the same information.

9.4. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

9.5. Where a SAR has been made electronically, the information will typically be provided in a commonly used electronic format. In most cases, a link to a secure Google Drive folder will be provided for a period of 48 hours in order for the requestor to download the information onto their device.

9.6. Where a SAR has been made for information held about a child, the school/academy will evaluate whether the child is capable of fully understanding their rights. If the school/academy determines the child can understand their rights, it will respond directly to the child.

9.7. All requests will be responded to without delay and at the latest, within one calendar month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by up to 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.

9.8. Where a request is manifestly unfounded or excessive, the Trust 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.

9.9. The Trust will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, the school/academy will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise. Documents will be presented in a redacted format as all details identifying any third parties will be redacted from the response
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent
- Explain to the individual who made the SAR why their request could not be responded to in full

9.10. In the event that a large quantity of information is being processed about an individual, the school/academy will ask the individual to specify the information the request is in relation to - the time limit for responding to the request will be paused until clarification from the individual is received.

10. The Right to Rectification

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

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

10.3. Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the Trust may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. The school/academy reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

10.4. The Trust will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. The Trust will restrict processing of the data in question whilst its accuracy is being verified, where possible.

10.5. Where the personal data in question has been disclosed to third parties, the school/academy will inform them of the rectification where possible. Where appropriate, the school/academy will inform the individual about the third parties that the data has been disclosed to.

10.6. Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, the school/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 Erasure

11.1. Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals, including children, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected or processed
- When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

11.2. The school/academy will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

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

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

11.4. The school/academy has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross border threats to health

- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services

11.5. Requests for erasure will be handled free of charge; however, the Trust may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

11.6. 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.

11.7. 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. Where personal data has been made public within an online environment, the school/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, including children, have the right to block or suppress the school/academy's processing of personal data.

12.2. The school/academy will restrict the processing of personal data in the following circumstances:

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

12.3. In the event that processing is restricted, the school/academy 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. The school/academy will inform individuals when a restriction on processing has been lifted.

12.4. Where the school/academy is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

12.5. If the personal data in question has been disclosed to third parties, the school/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.

12.6. The school/academy reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. 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.

13. The Right to Data Portability

13.1. Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:

- Where personal data has been provided directly by an individual to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

13.2. Personal data can be easily moved, copied or transferred from one Information and Communications Technology (ICT) environment to another in a safe and secure manner, without hindrance to usability. Personal data will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The school/academy will not be required to adopt or maintain processing systems which are technically compatible with other organisations. The school/academy will provide the information free of charge.

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

13.4. The school/academy will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the time frame 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.

13.5. Where no action is being taken in response to a request, the school/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 school/academy will inform individuals, including children, 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. Individuals, including children, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Processing used for direct marketing purposes
- Processing for purposes of scientific or historical research and statistics

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

- An individual's grounds for objecting must relate to his or her particular situation
- The school/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 school/academy can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The school/academy will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress

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

- The right to object is absolute and the school/academy will stop processing personal data for direct marketing purposes as soon as an objection is received
- The school/academy cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes
- The school/academy will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future

14.4. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object
- Where the processing of personal data is necessary for the performance of a public interest task, the school/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 school/academy will offer a method for individuals to object online.

14.6. The **DPO** will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings. The school/academy will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.

14.7. Where no action is being taken in response to an objection, the school/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.

15. Complaints

15.1. Complaints regarding how the Trust processes personal data and the management of data protection should be directed to the **DPO**.

15.2. **How can Data Subjects contact the individual(s) responsible for processing their personal data?**
The Trust's **DPO** can be contacted via the following means:

- **Telephone:** 01904 560053
- **Email:** dpo@hlt.academy
- **Postal Address:** FAO Data Protection Team, Heartwood Learning Trust, Rawcliffe Drive, Clifton (Without), York, YO30 6ZS

15.3. **How can Data Subjects submit a complaint if they are concerned about the handling of their personal data?**
Data Subjects can contact the **DPO** via the above contact details to discuss any concerns they may have in relation to the processing of their personal data. If the Data Subject is dissatisfied with how their complaint has been resolved, or believes their data has been mishandled, they are able to contact the **Information Commissioner's Office (ICO)** to raise their concerns.

15.4. The **ICO** is the UK's regulatory body for data protection and information rights, and is able to provide advice and guidance to the public and organisations. The **ICO** can be contacted via the following means:

- Accessing 'live chat' via their website here

- Completing the online complaints form here
- Contacting their helpline on 03031 231113 (Mon-Fri between 09:00-17:00)

16. Automated Decision Making and Profiling

16.1. The Trust will only ever conduct solely automated decision making with legal or similarly significant effects is the decision is:

- Necessary for entering into or performance of a contract
- Authorised by law
- Based on the individual's explicit consent

16.2. Automated decisions will not concern a child nor use special category personal data, unless:

- The school/academy has the explicit consent of the individual
- The processing is necessary for reasons of substantial public interest

16.3. The Trust will conduct a **DPIA** for automated decision making to mitigate risk of errors, bias and discrimination.

16.4. The school/academy will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

16.5. Individuals have the right not to be subject to a decision when both of the following conditions are met:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

16.6. The school/academy will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

16.7. When automatically processing personal data for profiling purposes, the school/academy will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact
- Using appropriate mathematical or statistical procedures
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects

17. Data Protection by Design and Default

17.1. The Trust will act in accordance with the **UK GDPR** by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, the school/academy will ensure that only data that is necessary to achieve its specific purpose will be processed.

17.2. The Trust will implement a data protection by design and default approach by using a number of

methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices
- Making data protection an essential component of the core functionality of processing systems and services
- Automatically protecting personal data in school/academy ICT systems
- Implementing basic technical measures within the Trust network and ICT systems to ensure data is kept secure
- Promoting the identity of the **DPO** and the **ESM** as a point of contact
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data

18. Data Protection Impact Assessments (DPIAs)

18.1. **DPIAs** will be used in certain circumstances to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy. **DPIAs** will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust's reputation which might otherwise occur. A **DPIA** will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and will be used for more than one project, where necessary.

18.2. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of Closed-Circuit Television (CCTV)

18.3. The Trust will ensure that all **DPIAs** include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

18.4. Where a DPIA indicates high risk data processing, the **DPO/ESM** will consult the **ICO** to seek its opinion as to whether the processing operation complies with the **UK GDPR**.

19. Data Breaches

19.1. Please refer to the Trust's **Data Breach Policy and Procedures** for more information regarding how the Trust responds to data breaches.

19.2. 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. The **Principal**, supported by the school/academy **GDPR Representative**, will ensure that employees are made aware of, and understand, what constitutes a data breach as part of their training.

19.3. Effective and robust breach detection, investigation and internal reporting procedures are in place at the school/academy, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

19.4. Where the school/academy faces a data security incident, the **DPO**/**ESM** will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

19.5. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school/academy becoming aware of it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. 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. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

19.6. Within a breach notification to the supervisory authority, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the **DPO**/**ESM**
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

19.7. When notifying an individual about a breach to their personal data, the school/academy will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

19.8. The **DPO**/**ESM**, supported by the school/academy **GDPR Representative**, will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the **UK GDPR** accountability principle and in accordance with the Trust's **Data Breach Policy and Procedures**.

19.9. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

19.10. The Trust will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error and/or developing strategies with the external IT provider to improve the security of the wider ICT systems.

20. Data Security

20.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access, and will not be left unattended or in clear view anywhere with general access.

20.2. 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. Removable data storage devices are not permitted. Memory sticks will not be used to hold personal information. All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

20.3. Employees are not permitted to use their personal devices for work purposes unless this is for formal two factor factor authentication i.e. authentication purposes via an official app i.e. Google Authenticator or Microsoft Authenticator. Employees are provided with a secure login and password, and devices will regularly prompt users to change their password.

20.4. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Circular emails to parents/carers are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. When sending confidential information employees **must** check that the recipient is correct before sending. Failure to comply with these requirements may result in personal data breaches.

20.5. All Trustees and Governors are required to use a Trust email account for all governance related matters. Trustees and Governors are issued with an account upon the successful completion of the required safeguarding and DBS checks. Access to the online governance portal is password protected and is governed by a separate **DPIA**.

20.6. Before sharing personal data, employees will ensure:

- They are allowed to share it
- That adequate security measures are is in place to protect it
- Who will receive the data has been outlined in the applicable **Privacy Notice(s)**

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

20.8. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school/academy containing sensitive information are supervised at all times.

20.9. The physical security of the school/academy's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism, burglary or theft is identified, extra measures to secure data storage will be put in place.

20.10. The school/academy will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.

20.11. The school/academy takes its duties under the **UK GDPR** seriously and any unauthorised disclosure may result in disciplinary action. The **GDPR Representative**, supported by the **Principal**, is responsible for continuity and recovery measures are in place to ensure the security of protected data.

20.12. When disposing of data, paper documents will be shredded and digital storage devices will be physically destroyed when they are no longer required. ICT assets will be disposed of in accordance with the **ICO**'s guidance on the disposal of ICT assets. Please refer to the Trust's **Assets and Disposals Policy**.

20.13. The Trust holds the right to take the necessary disciplinary action against an employee if they believe

them to be in breach of the above security measures.

21. Safeguarding

21.1. The Trust understands that the **UK GDPR** does not prevent or limit the sharing of information for the purposes of keeping children safe.

21.2. The school/academy will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the **Designated Safeguarding Lead (DSL)** will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent/carer
- The reason that consent has not been sought, where appropriate

21.3. The school/academy will aim to gain consent to share information where appropriate and where doing so would not place a child at risk. The school/academy will manage all instances of data sharing for the purposes of keeping a child safe in line with the Trust's **Safeguarding and Child Protection Policy**.

21.4. Pupils' personal data will not be provided where the serious harm test is met. Where there is doubt, the school/academy will seek advice from the **DPO**.

22. Publication of Information

22.1. The Publication Scheme can be found within the Trust's **Freedom of Information Policy**, which is available via the Trust website and outlines classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

22.2. Classes of information specified in the **Publication Scheme** are made available quickly and easily on request.

22.3. The school/academy will not publish any personal information, including photos, on its website without the permission of the affected individual. At the start of each academic year the school/academy requires all parents/carers to complete a consent form which clearly explains to parents/carers the reasons why and how the school/academy uses images and videos of pupils.

22.4. Parents/carers are advised that without their consent the school/academy will not use images and videos of children. When uploading information to the school/academy website, employees are considerate of any metadata or deletions which could be accessed in documents and images on the site. Please refer to the Trust's **Photography and Videos at School Policy** for further information and to

access a copy of a consent form template.

23. CCTV and Photography

23.1. The Trust provides each school/academy with a model **CCTV Policy** which is adapted to suit each local setting where CCTV is in operation. Please refer to the individual school/academy **CCTV Policy** (where applicable), available on the school/academy website. Pupils, employees and visitors are advised that CCTV is in operation, via external signage.

23.2. The school/academy understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.

23.3. The school/academy notifies all pupils, employees and visitors of the purpose for collecting CCTV images via notice boards, letters and email. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All CCTV footage will be kept in line with the Trust's **CCTV Policy** for security purposes; the **Principal** is responsible for keeping the records secure and permitting access. Access to the CCTV system and the recordings is limited; please refer to the **CCTV Policy** for further information.

23.4. Before the school/academy is able to obtain the data of pupils or employees, it is required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the **Protection of Freedoms Act 2012**.

23.5. The school/academy will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them. The school/academy obtains annual consent from parents/carers for the use of images or video footage of pupils, via a parental consent form. The form details where the image/video will be used, for instance: in a publication, such as the Trust/school/academy website, school/academy prospectus, for social media use or for marketing purposes, and so on. Precautions, as outlined in the Trust's **Photography and Videos at School Policy**, are taken when publishing photographs of pupils, in print, video or on the school/academy website.

23.6. Images captured by individuals for recreational or personal purposes, and videos made by parents/carers for family use, are exempt from the **UK GDPR.**

23.7. Parents/carers and others attending school/academy events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents/carers or visitors to the school/academy.

23.8. The school/academy asks that parents/carers and others do not post any images or videos which include any child other than their own child(ren) on any social media or otherwise publish those images or videos.

24. Cloud Computing

24.1. For the purposes of this policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the Trust/school/academy accessing a shared pool of ICT services remotely via a private network or the internet (e.g. via a shared Google Drive).

24.2. Employees will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

24.3. If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when their employment with the Trust/school/academy ends.

24.4. All files and personal data will be encrypted before they leave a Trust/school/academy operated device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the **DPO** immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

24.5. As with files on Trust/school/academy operated devices, only authorised parties will be able to access files on the cloud.

24.6. The Trust/school/academy's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the **DPO**. The **DPO** will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the **UK GDPR** and **DPA**. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

24.7. The **DPO** will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the Trust's **Data Protection (UK GDPR) Policy**
- Confirm that the service provider will remove all copies of data, including back-ups, if requested
- Find out what will happen to personal data should the Trust decide to withdraw from the cloud service in the future
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk

25. Data Retention

25.1. Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable.

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

25.3. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained. Volume deletion of electronic files, based on request by the Trust/school/academy, will be carried out by our IT partner, via an agreed and scheduled process.

26. DBS Data

26.1. All data provided by the Disclosure and Barring Service (DBS) will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated.

26.2. 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.

27. Monitoring and Review

27.1. The approver of this policy and the next scheduled review date is shown on the cover page of this document.

Appendix A - Data Retention Schedule

The following **Data Retention Schedule** has been updated and reviewed alongside the **Information and Records Management Society (IRMS) Toolkit** guidance and the **Academy Trust Handbook (2022)**.

Heartwood Learning Trust is committed to maintaining the confidentiality of its information and ensuring that all records are only accessible to the appropriate individuals. In line with the requirements of the **UK GDPR**, the Trust also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

For the purposes of this data retention schedule, the term "SECURE DISPOSAL" refers to permanent destruction of the information by shredding, pulping or burning, for example.

At the time of writing, the following data retention schedule should be considered up to date with current legislation for schools/academies; however this will be periodically reviewed in line with the Trust's **Data Protection (UK GDPR) Policy** review period.

Pupil records and other pupil-related information

The table below outlines the Trust's retention periods for individual pupil records and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will be destroyed in line with the retention periods below.

Pupil Records				
1. Personal identifiers and characteristics				
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Images used for identification purposes		For the duration of the event/activity, or whilst the pupil remains at school, whichever is less, plus one month	SECURE DISPOSAL
b.	Images used in displays		Whilst the pupil is at school	SECURE DISPOSAL
c.	Images used for marketing purposes		In line with the consent period	SECURE DISPOSAL
d.	Biometric data		For the duration of the event/activity, or whilst the pupil remains at school, whichever is less	SECURE DISPOSAL
2. Admissions				
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Register of Admissions	● School Attendance: Departmental Advice 2014 ● School Admissions Code 2014 ● **Guidance:** Working together to improve school attendance 2022	Retained for a minimum of 3 years from the date of the most recent entry	Consider transfer to archives
b.	Admissions – If the admission is successful	School Admissions Code 2014	Admission + 1 year	SECURE DISPOSAL
c.	Admission – if the appeal is unsuccessful	School Admissions Code 2014	Resolution of case + 1 year	SECURE DISPOSAL

d.	Secondary transfer sheets (Primary)	School Admissions Code 2014	Current year + 2 years	SECURE DISPOSAL
e.	Proofs of address supplied by parents/carers as part of the admissions process	School Admissions Code 2014	Retained for 1 year following the current academic year	SECURE DISPOSAL
f.	Supplementary information (e.g. religion, medical conditions etc) - For successful admissions	School Admissions Code 2014	This information should be included within the pupil file as retained as such	SECURE DISPOSAL
g.	Supplementary information (e.g. religion, medical conditions etc) - For unsuccessful admissions	School Admissions Code 2014	Information retained until an appeals process is completed or until the deadline for requesting an appeal has passed	SECURE DISPOSAL
3.	**Educational Records**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Primary School Pupil Files	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No 1437	Files should be retained for the duration of the pupil's attendance at the school/academy establishment	Files should be transferred to another primary school, secondary school or pupil referral unit when the child leaves school. If the child dies whilst enrolled, transfers to an independent school, leaves the country or is home schooled, their file is returned to the LA
b.	Secondary School Pupil Files/Educational Record	● Keeping Children Safe in Education 2025 ● The Report of the Independent Inquiry into Child Sexual Abuse 2022 (p105)	Date of birth of the pupil + 50 years (this is to aid any investigations into historical sexual abuse that may be reported after the pupil has left school)	SECURE DISPOSAL
c.	Examination Results		Retained within the pupil file. Pupils will be asked to collect any certificates by the end of the current	All uncollected certificates should be returned to the

			academic year	examination board at the end of each academic year
d.	Internal examination results (e.g. mock exams, school/progress tests)		Added to the pupil file	Other copies (not retained in pupil file) will be subject to SECURE DISPOSAL
e.	Behaviour records		Added to the pupil file	SECURE DISPOSAL
f.	Suspension/Exclusion records		Added to the pupil file	SECURE DISPOSAL
g.	Pupils' work		This should be returned to the pupil at the end of each academic year. Where pupil's work is not accepted, this should be retained for 1 year after this date and returned to the pupil if requested	SECURE DISPOSAL
h.	Careers advice and subsequent agreed decisions		Whilst the pupil is at the school, plus three years	SECURE DISPOSAL
i.	Education, training or employment destinations data		Whilst the pupil is at the school, plus three years	SECURE DISPOSAL
j.	Statement maintained under The Education Act 1996 and any amendments made to statement	● Education Act 1996 ● Special Educational Needs and Disability Act 2001 (section 1)	This is usually retained within the pupil file, but otherwise will be retained until the pupil reaches the age of 25	SECURE DISPOSAL unless legal action is pending
4.	**Attendance**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Attendance registers	**Guidance:** Working together to improve school attendance 2022	Retained for 3 years from the date of entry onto the register	SECURE DISPOSAL
b.	Correspondence relating to any absence (authorised or unauthorised)	Education Act 1996 Section 7	Retained for 2 years following the current academic year	SECURE DISPOSAL
c.	Correspondence relating to Authorised Absence Issues	● Education Act 1995 (s7) ● Children Missing Education 2016	Retained for 3 years from the date of absence/register	SECURE DISPOSAL

		• **Guidance:** Working together to improve school attendance 2022		
5.	**Medical Information**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Permission slips for administering medication		For the duration of the period that medication is given, plus one month	SECURE DISPOSAL
b.	Medical conditions – ongoing management		Added to the pupil's record	SECURE DISPOSAL
c.	Medical incidents that have a behavioural or safeguarding influence		Added to the pupil's record	SECURE DISPOSAL
6.	**SEND Information**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Accessibility Strategy	• Special Educational Needs and Disability Act 2001 (section 14) • Equality Act 2010	This is usually retained within the pupil file, but otherwise will be retained until the pupil reaches the age of 25	SECURE DISPOSAL unless legal action is pending
b.	Advice and information to parents regarding educational needs	Special Educational Needs and Disability Act 2001 (section 2)	This is usually retained within the pupil file, but otherwise will be retained until the pupil reaches the age of 25	SECURE DISPOSAL unless legal action is pending
c.	Special Educational Needs Files, reviews and IEPs	• Limitation Act 1980 • Working Together to Safeguard Children 2020 • Keeping Children Safe in Education 2025 • The Special Educational Needs and Disability Regulations 2014	Retained for a minimum of 25 years from the DOB of the Pupil. It is recommended that files relating to SEN be retained for a longer period (up to 50 years) to defend against any "failure to provide a sufficient education" cases which may arise at a later date.	Review once the pupil reaches the age of 25. In the event a pupil transfers to another school, their IEP should be transferred alongside their pupil file within 15 working days

7.	Curriculum Management			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	SATS Results		Results will be retained within the pupil's educational file. The school/academy may retain a record of whole year group SATs results for comparison purposes for 6 years following the current academic year	SECURE DISPOSAL
b.	Examination papers		Examination papers should be retained until any appeals/validation process is complete, or until the deadline for submitting an appeal request has passed (typically 14 days after a preliminary result is released by the exam board)	SECURE DISPOSAL
c.	Published Admission Number (PAN) reports		Current academic year + 6 years	SECURE DISPOSAL
d.	Value Added and Contextual Data		Current academic year + 6 years	SECURE DISPOSAL
e.	Self Evaluation forms		Current academic year + 6 years	SECURE DISPOSAL
8.	**Educational Visits and Trips**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Parental consent forms for school trips – where there has been no major incident	Limitation Act 1980 (Section 2)	Conclusion of the trip	SECURE DISPOSAL
b.	Parental consent forms for school trips – where there has been a major incident	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The Permission slips for all pupils on the trip need to be retained to show that the rules had been followed for	SECURE DISPOSAL

			all pupils	
c.	Records created by Primary schools to obtain approval to run an Educational Visit	• Outdoor Education Advisers' Panel National Guidance: http://oeapng.info (Sections 3-4) • Health & Safety of Pupils on Educational Visits (HASPEV) (1998)	Date of visit + 14 years	SECURE DISPOSAL
d.	Records created by Secondary schools to obtain approval to run an Educational Visit	• Outdoor Education Advisers' Panel National Guidance: http://oeapng.info (Sections 3-4) • Health & Safety of Pupils on Educational Visits (HASPEV) (1998)	Date of visit + 10 years	SECURE DISPOSAL
e.	Educational visitors in school – sharing of personal information		Until the conclusion of the visit, plus one month	SECURE DISPOSAL
f.	Walking Bus registers		Date of register + 3 years (this takes into account the period of time required for accident reporting, if required)	SECURE DISPOSAL
g.	Work experience agreement		DOB of child + 18 years	SECURE DISPOSAL
9.	**Family Liaison Officers and Home-School Liaison Assistants**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Day Books		Retained for 2 years following the current academic year	SECURE DISPOSAL
b.	Reports for outside agencies – where the report has been included on the case file created by the outside agency		Retained whilst the pupil is enrolled at the school/academy	SECURE DISPOSAL
c.	Referral forms		Retained whilst the referral is 'current' and the pupil is still receiving support from the outside agency	SECURE DISPOSAL
d.	Contact data sheets/database		Retained for the current academic year and then reviewed. Retained for a further academic year if	SECURE DISPOSAL

			outside agency support is ongoing and then reviewed again	
e.	Group Registers		Retained for 2 years following the current academic year	SECURE DISPOSAL
10. Catering and Free School Meals (FSM)				
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Meal administration		Whilst the pupil is at school + 1 year	SECURE DISPOSAL
b.	Free School Meal eligibility		Whilst the pupil is at school + 5 years	SECURE DISPOSAL
c.	School meals register		Current academic year + 3 years	SECURE DISPOSAL
d.	Free school meals register		Current academic year + 6 years	SECURE DISPOSAL
e.	School Meals Summary Sheets		Current academic year + 3 years	SECURE DISPOSAL
11. Child Protection				
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Child Protection files (Including Children In Care (CIC) & Children Previously In Care (CPIC))	● Keeping Children Safe in Education 2025 ● The Report of the Independent Enquiry into Child Sexual Abuse 2022 (p177)	Date pupil leaves the school + 50 years (this is to allow sufficient time to report any historical abuse and for Police investigations to not be hindered by removal of records)	SECURE DISPOSAL
b.	Allegation of a child protection nature against a member of staff which is proven to be false or malicious, including where the allegation is unfounded	● The Report of the Independent Enquiry into Child Sexual Abuse 2022 (p126) ● Working Together to Safeguard Children 2018 (p60) ● Keeping Children Safe in Education 2025	False or malicious allegations should be retained on the pupil's record until the pupil leaves the school/academy. False or malicious allegations relating to Child Sexual Abuse should be retained on the member of staff's	SECURE DISPOSAL

		● **Guidance**: Dealing with Allegations of Abuse against Teachers and Other Staff 2012 (p28) ● Employment Practices Code 2011 (s2.13)	personnel file until they leave the school/academy.	
c.	Child protection information held in separate files	● Keeping Children Safe in Education 2025 ● Working Together to Safeguard Children 2020	Retained until the pupil reaches the age of 25 years, and then reviewed. This was agreed in consultation with the Safeguarding Children Group on the basis that the principal copy will be found on the LA Social Services Record	SECURE DISPOSAL

Employee Records

The table below outlines the school's retention period for staff records and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Employee Records				
1. Operational				
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Staff Members' Personnel files	Limitation Act 1980 (Section 2)	Retained for 6 years following cessation of employment	SECURE DISPOSAL
b.	Annual appraisal/assessment records		Current academic year + 5 years	SECURE DISPOSAL
c.	Records relating to pay and conditions	Limitation Act 1980	Retained for 6 years following the date pay agreements/conditions are superseded Retained for 6 years following cessation of employment	SECURE DISPOSAL
d.	Maternity pay records	Statutory Maternity Pay (General) Regulations 1986 (and subsequent amendments)	Retained for 3 years following the current academic year	SECURE DISPOSAL
e.	Records held under Retirement Benefits Schemes (information powers) regulations 1995	● The Pension Schemes Act 2021 ● Pensions Act 2014	Current academic year + 6 years	SECURE DISPOSAL
f.	Sickness absence monitoring (where sickness pay is not paid)		Current academic year + 3 years	SECURE DISPOSAL
g.	Sickness absence monitoring (where sickness pay is paid)		Current academic year + 6 years	SECURE DISPOSAL
h.	Staff training		Retained in the personnel file	SECURE DISPOSAL
2. Recruitment				

	Basic File Description	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
a.	Interview notes and recruitment notes		Date of interview + 6 months	SECURE DISPOSAL
b.	Records leading up to the appointment of a Principal		Date of appointment + 6 years	SECURE DISPOSAL
c.	All records leading up to the appointment of a new employee – unsuccessful candidates		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
d.	All records leading up to the appointment of a new employee - successful candidate		All relevant information should be added to the personnel file and supplementary information retained for a further 6 months	SECURE DISPOSAL
e.	Records of DBS checks (forms part of the pre-employment vetting procedure)	● Keeping Children Safe in Education 2025 ● UK GDPR and DPA 2018 Article 10	The Trust is not required to retain copies of DBS certificates. Copies of DBS certificates/records of disclosed criminal information must not be retained for longer than 6 months from the date of verification. Signed and dated records of verification of DBS checks should be retained for the duration of employment on the SCR	SECURE DISPOSAL (e.g. shredding, pulping or burning)
f.	Proof of identity as part of the enhanced DBS check		If it is necessary to keep a copy, it will be held within the personnel file	SECURE DISPOSAL
g.	Evidence proving the right to work in the UK (forms part of the pre-employment vetting procedure)	An Employer's Guide to Right to Work Checks (Home Office May 2015)	Where possible these documents should be retained within the personnel file. If retained separately they should be retained for 2 years following cessation of employment	SECURE DISPOSAL
3.	**Disciplinary and Grievance**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**

a.	Child protection allegations, including where the allegation is unproven	• Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) • Education Act 2002 Guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Added to personnel file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer If allegations are malicious, they are removed from personnel files with immediate effect If allegations are found, they are kept on the personnel file and a copy is provided to the person concerned unless the member of staff is part of any case which falls under the terms of reference of the IICSA. If this is the case, the file is retained until IICSA enquiries are complete	SECURE DISPOSAL
b.	Oral warnings		Date of warning, plus 6 months	SECURE DISPOSAL
c.	Written warning – level 1		Date of warning, plus 6 months	SECURE DISPOSAL
d.	Written warning – level 2		Date of warning, plus 12 months	SECURE DISPOSAL
e.	Final warning		Date of warning, plus 18 months	SECURE DISPOSAL
f.	Case not found following disciplinary procedure		Records relating to other matters should be disposed of immediately following conclusion of the case	SECURE DISPOSAL

Governance Records

The table below outlines the Trust's retention periods for governance records, and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Governance Records				
1. Governance				
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Agendas		One copy to be retained with the master copy of minutes. Otherwise agendas should be retained for the duration of the meeting.	SECURE DISPOSAL
b.	Signed Minutes (master copy)	Companies Act 2006 (s248, s355)	At least 10 years from the date of the meeting	Permanent storage in external archive (e.g. County Archives Service)
c.	Minutes for Inspection	Companies Act 2006 (s248) - Minutes should be redacted if they contain any personal information about staff members/pupils	3 years from the date of the meeting	SECURE DISPOSAL
d.	Unsigned Minutes		Retained for the duration of the meeting only	SECURE DISPOSAL
e.	Reports Presented to the Governing body		Minimum of 6 years from the date of presentation. If the minutes of the meeting make reference to the report, the report should then be retained alongside the master copy of minutes	SECURE DISPOSAL or retain with signed set of minutes
f.	Meeting papers relating to the annual parents' meeting	Education Act 2002 (s33) - now superseded by Education Act 2011	6 years from the date of the meeting	SECURE DISPOSAL
g.	Instruments of Government including Articles of Association	Companies Act 2006	PERMANENTLY	Permanent storage with the Trust or in external archive

				(e.g. County Archives Service)
h.	Trusts and Endowments managed by the Governing Body		PERMANENT	Retain whilst operationally required then offered to County Archives
i.	Action Plans		Retained for 6 years after the date the plan is superseded	SECURE DISPOSAL
j.	Statutory Policy Documents (e.g. Data Protection, Freedom of Information, SEND, Complaints, Equality Objectives etc)		Retained for 6 years after the policy is superseded (this should cover any operational need including any previous decision-making processes)	SECURE DISPOSAL
k.	Records relating to **complaints** dealt with by the Trust Board	● Education and Inspections Act 2006 (s160) ● The Complaints against Schools (England) Regulations 2010 ● Education Act 2002 (s29)	Retained for 6 years after the 'resolution' of the complaint. If negligence is involved, records are retained for the current academic year, plus 15 years If child protection or safeguarding issues are involved, the records are retained for the current academic year, plus 40 years	SECURE DISPOSAL
l.	Annual reports required by the DfE	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	Date of report, plus 10 years	SECURE DISPOSAL
m.	Proposals for change of status of a maintained school including specialist status schools and academies		Retained for 3 years after the proposal is accepted or declined	SECURE DISPOSAL
n.	Scheme of delegation and terms of reference for committees		Until superseded or whilst relevant	Standard disposal
o.	Meeting schedule		Current academic year	Standard disposal
p.	Register of attendance at full governing board meetings		Date of last meeting, plus six years	SECURE DISPOSAL
q.	Records relating to governor monitoring visits		Date of the visit, plus three years	SECURE DISPOSAL

r.	All records relating to the conversion of the school to academy status		Permanent	Local archives are consulted before disposal
s.	Records relating to the terms of office of serving governors, including evidence of appointment		Date on which the governor's appointment ends, plus six years	SECURE DISPOSAL
t.	Records relating to governor declaration against disqualification criteria		Date on which the governor's appointment ends, plus six years	SECURE DISPOSAL
u.	Register of business interests		Date the governor's appointment ends, plus six years	SECURE DISPOSAL
v.	Trustee and Governor code of conduct		Until superseded or whilst relevant	SECURE DISPOSAL
w.	Trustee/Governor personnel files		Date on which the governor's appointment ends, plus six years	SECURE DISPOSAL
2.	**Member, Trustee and Governor Recruitment**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Governors' personal details (e.g. name, occupation, correspondence address and date + month of birth)	● Companies Act 2006 (s113) ● **Guidance:** Companies House Register	Dissolved company records can be transferred to the National Archive, if this is not possible, Companies House are responsible for secure disposal	Dissolved company records can be transferred to the National Archive, if this is not possible, Companies House are responsible for secure disposal
b.	Trustees' personal details (e.g. name, occupation, correspondence address and date + month of birth)	● Companies Act 2006 (s113) ● **Guidance:** Companies House Register	Retained by Companies House on the Statutory Public Register from the date of appointment, until such time as the Trust is dissolved and records are retained 20 years thereafter	Dissolved company records can be transferred to the National Archive, if this is not possible, Companies House are responsible for secure disposal
c.	Records relating to the induction programme for new Trustees/Governors		Date on which the appointment ends, plus six years	SECURE DISPOSAL

3. Heartwood Learning Trust				
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Governance statement		Life of governance statement, plus six years	SECURE DISPOSAL
b.	Articles of association		Life of the academy	SECURE DISPOSAL
c.	Memorandum of understanding		Can be disposed of once the academy has been incorporated	SECURE DISPOSAL
d.	Memorandum of understanding of shared governance among schools		Life of memorandum of understanding, plus six years	SECURE DISPOSAL
e.	Constitution		Life of the academy	SECURE DISPOSAL
f.	Special resolutions to amend the constitution		Life of the academy	SECURE DISPOSAL
g.	Written Scheme of Delegation	Companies Act 2006 (s355)	Retained for 10 years after the 'life' of the scheme	SECURE DISPOSAL
h.	Directors – appointment		Life of appointment, plus six years	SECURE DISPOSAL
i.	Directors – disqualification		Data of disqualification, plus 15 years	SECURE DISPOSAL
j.	Directors – termination of office		Date of appointment, plus six years	SECURE DISPOSAL
k.	Annual trustee report		Date of report, plus 10 years	SECURE DISPOSAL
l.	Annual report and accounts		Date of report, plus 10 years	SECURE DISPOSAL
m.	Annual return		Date of report, plus 10 years	SECURE DISPOSAL
n.	Statement of Trustees' responsibilities		Life of appointment, plus six years	SECURE DISPOSAL
o.	Strategic review		Date of review, plus six years	SECURE DISPOSAL

p.	Register of directors		Life of academy, plus six years	SECURE DISPOSAL
q.	Register of directors' interests		Life of academy, plus six years	SECURE DISPOSAL
r.	Register of directors' residential addresses		Life of academy, plus six years	SECURE DISPOSAL
s.	Register of gifts/hospitality	Companies Act 2006	Retained for the life of the Trust + 6 years thereafter	SECURE DISPOSAL
t.	Register of Members	Companies Act 2006	Retained for the life of the Trust + 6 years thereafter	SECURE DISPOSAL
u.	Register of Secretaries	Companies Act 2006	Retained for the life of the Trust + 6 years thereafter	SECURE DISPOSAL
v.	Register of Trustees' Interests		Retained for the life of the Trust + 6 years thereafter	SECURE DISPOSAL
w.	Declaration of Interests Statements (Governors)		Retained for the life of the Trust + 6 years thereafter	SECURE DISPOSAL

Leadership and Management Records

The table below outlines the school's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Management Information				
1. Principal and SLT				
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Log Books of activity in the school/academy		Retained for 6 years (and then reviewed) from the date of the last entry	Offered to County Archives
b.	Minutes of the SLT and other internal administrative bodies		Retained for 3 years (and then reviewed) following the date of the meeting	SECURE DISPOSAL
c.	Reports created by the Principal or SLT		Date of the report, plus a minimum of three years	SECURE DISPOSAL
d.	Records created by members of the SLT or staff with administrative responsibilities		Retained for 3 years following the current academic year (and then reviewed)	SECURE DISPOSAL
e.	Correspondence created by members of the SLT or staff with administrative responsibilities		Retained for 3 years (and then reviewed) following the date of correspondence	SECURE DISPOSAL
f.	Professional Development Plans		Retained for 6 years following the 'life' of the plan	SECURE DISPOSAL
g.	All records relating to the creation and implementation of School Admissions policy	School Admissions Code Dec 2014	Retained for 3 years following the policy being superseded	SECURE DISPOSAL
2. Curriculum				

	Basic File Description	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
a.	School Development Plan		Current academic year + 6 years	SECURE DISPOSAL
b.	Curriculum returns		Current academic year + 3 years	SECURE DISPOSAL
c.	Schemes of work		Current academic year + 1 year	SECURE DISPOSAL
d.	Timetable		Current academic year + 1 year	SECURE DISPOSAL
e.	Class record books		Current academic year + 1 year	SECURE DISPOSAL
f.	Mark Books		Current academic year + 1 year	SECURE DISPOSAL
g.	Record of homework set		Current academic year + 1 year	SECURE DISPOSAL
h.	Examination results (school/academy copy)		Current academic year + 6 years	SECURE DISPOSAL

Health and Safety Records

The table below outlines the Trust's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Health and Safety				
1. Health and Safety				
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Accessibility Plans	● Equality Act 2010 (Schedule 10) ● Disability Discrimination Act	Retained for 6 years after the 'life' of the plan	SECURE DISPOSAL
b.	Health and Safety Policies and Procedures		Retained for 3 years following expiry of the document	SECURE DISPOSAL
c.	Generic H&S Risk Assessments (RAs)		Retained whilst the RA is in use and for a further 3 years	SECURE DISPOSAL
d.	Records relating to any reportable death, injury, disease or dangerous occurrence under RIDDOR		Date of incident + 12 years	SECURE DISPOSAL
e.	Accident Reporting	● Social Security (Claims and Payments) regulations 1979 (reg. 25) Social Security Administration Act 1992 (section 8) ● Limitation Act 1980	Accident books must be retained for 3 years following the last entry Incident reporting forms (adults) should be retained for 6 years following the date of the incident. Forms for pupils should be retained until they reach the age of 25 years	SECURE DISPOSAL
f.	Control of Substances Hazardous to Health (COSHH) records	● Control of Substances Hazardous to Health Regulations 2002 (regulation 11) Health and Safety Executive advice	Current academic year + 40 years	SECURE DISPOSAL
g.	Process of monitoring of areas where	Control of Asbestos at Work Regulations 2012	Retained for 40 years following the most recent action	SECURE DISPOSAL

	employees and persons are likely to have become in contact with asbestos	(Regulation 19)	taken regarding asbestos monitoring	
h.	Process of monitoring of areas where employees and persons are likely to have come into contact with radiation	The Ionising Radiations Regulations 2017	Retained for 50 years following the most recent action taken regarding radiation monitoring	SECURE DISPOSAL
i.	Fire Precautions log books	The Regulatory Reform (Fire Safety) Order 2005	Current academic year + 6 years	SECURE DISPOSAL
j.	Fire Risk Assessment	The Regulatory Reform (Fire Safety) Order 2005	Retained for the 6 years from the date the RA is no longer in use	SECURE DISPOSAL
k.	Health and safety file to show current state of buildings, including all alterations (wiring, plumbing, building works etc.) to be passed on in the case of change of ownership		Permanent	Passed to new owner on sale or transfer of building
2.	**Property Management**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Workplace Inspections	Health and Safety at Work etc. Act 1974	Current academic year + 3 years (then may be reviewed by the competent person or Trust Operations Manager)	SECURE DISPOSAL
b.	Title Deeds of properties belonging to the Trust		PERMANENT - Until such time as the property is sold	These should follow the property unless the property has been registered at the Land Registry
c.	Plans of property owned by the Trust		PERMANENT - Until such time as the property is sold	These should be passed on if the building is leased or sold to another party
d.	Leases of property by or to the Trust		Expiry of lease + 6 years	SECURE DISPOSAL

e.	Records relating to the letting of any Trust premises		Current financial year + 6 years	SECURE DISPOSAL
f.	Burglary, theft and vandalism report forms		Current academic year + 6 years	SECURE DISPOSAL
3.	**Property Maintenance**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Maintenance and contractors	Financial Regulations	Current academic year + 6 years	SECURE DISPOSAL
b.	Maintenance Log books (including works completed by employees)		Current academic year + 6 years	SECURE DISPOSAL

Retention of Financial Records

The table below outlines the school's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Financial Management				
1. Payroll and Pensions				
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Maternity pay records	Financial Regulations	Current academic year, plus three years	SECURE DISPOSAL
b.	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL
c.	Absence record	Financial Regulations	Current academic year, plus three years	SECURE DISPOSAL
d.	Batches	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL
e.	Car mileage claims	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL
f.	Elements	Financial Regulations	Current academic year, plus two years	SECURE DISPOSAL
g.	Income tax form P60	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL
h.	National insurance – schedule of payments	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL
i.	Overtime	Financial Regulations	Current academic year, plus three years	SECURE DISPOSAL
j.	Part-time fee claims	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL
k.	Payroll awards	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL

l.	Payroll (gross/net weekly or monthly)	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL
m.	Payroll reports	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL
n.	Payslips (copies)	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL
o.	Pension payroll	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL
p.	Personal bank details	Financial Regulations	Until superseded, plus three years	SECURE DISPOSAL
q.	Timesheets and records of sick pay	Financial Regulations	Retained for 6 years following the current academic year	SECURE DISPOSAL
r.	Staff returns	Financial Regulations	Current academic year, plus three years	SECURE DISPOSAL
s.	Superannuation adjustments	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL
t.	Tax forms	Financial Regulations	Current academic year, plus six years	SECURE DISPOSAL
2.	**Risk Management and Insurance**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Employer's Liability Insurance certificate		Retained for 40 years after such time as the school/academy closes	SECURE DISPOSAL
b.	Business continuity and disaster recovery plans		Retained for the 'life' of the plan + 3 years	SECURE DISPOSAL
3.	**Asset Management**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Inventories of equipment and		Retained for 6 years after the current academic year	SECURE DISPOSAL

	furniture			
4.	**Accounts and Statements**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Annual accounts		Current financial year + 6 years	STANDARD DISPOSAL
b.	Loans and Grants		Date of last payment on loan + 12 years (then reviewed)	SECURE DISPOSAL
c.	All records relating to the creation and management of budgets including the Annual Budget statement and background papers		Life of the budget + 3 years	SECURE DISPOSAL
d.	Invoices, receipts, order books, requisitions and delivery notices	Financial Regulations	Current financial year + 6 years	SECURE DISPOSAL
e.	Records relating to the collection and banking of monies		Current financial year + 6 years	SECURE DISPOSAL
f.	Records relating to the identification and collection of debt	Limitation Act 1980	Current financial year + 6 years	SECURE DISPOSAL
5.	**Contract Management**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Service level agreements (SLA)		Until superseded by another SLA	SECURE DISPOSAL
b.	Records relating to the management of contracts under seal	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
c.	Records relating to the management of	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL

	contracts under signature			
d.	Records relating to the monitoring of contracts		Current financial year + 2 years	SECURE DISPOSAL
e.	Records relating to the management of contracts with external providers (e.g. catering/cleaning provision)		Retained for 6 years from the date of the expiration date of the contract	SECURE DISPOSAL
6.	**School Fund**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Cheque books	Financial Regulations	Current academic year + 6 years	SECURE DISPOSAL
b.	Paying in books	Financial Regulations	Current academic year + 6 years	SECURE DISPOSAL
c.	Ledgers	Financial Regulations	Current academic year + 6 years	SECURE DISPOSAL
d.	Invoices	Financial Regulations	Current academic year + 6 years	SECURE DISPOSAL
e.	Receipts	Financial Regulations	Current academic year + 6 years	SECURE DISPOSAL
f.	Bank statements	Financial Regulations	Current academic year + 6 years	SECURE DISPOSAL
g.	Journey books	Financial Regulations	Current academic year + 6 years	SECURE DISPOSAL
h.	Student Grant applications	Financial Regulations	Current academic year + 3 years	SECURE DISPOSAL
i.	Petty cash books	Financial Regulations	Current academic year + 6 years	SECURE DISPOSAL
7.	**School Meals**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the**

				record
a.	FSM registers (where the register is used as a basis for funding)		Current academic year, plus six years	SECURE DISPOSAL
b.	School meals registers		Current academic year, plus three years	SECURE DISPOSAL
c.	School meals summary sheets		Current academic year, plus three years	SECURE DISPOSAL
8.	**Pupil Finance**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Student grant applications		Current academic year, plus three years	SECURE DISPOSAL
b.	Pupil premium fund records		Date the pupil leaves the school, plus six years	SECURE DISPOSAL
9.	**Trust Financial Records**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	Statement of financial activities for the year	Financial Regulations	Current financial year, plus six years	SECURE DISPOSAL
b.	Financial planning	Financial Regulations	Current financial year, plus six years	SECURE DISPOSAL
c.	Value for money statement		Current financial year, plus six years	SECURE DISPOSAL
d.	Records relating to the management of VAT		Current financial year, plus six years	SECURE DISPOSAL
e.	Whole of government accounts return		Current financial year, plus six years	SECURE DISPOSAL
f.	Borrowing powers		Current financial year, plus six years	SECURE DISPOSAL

g.	Budget plan		Current financial year, plus six years	SECURE DISPOSAL
h.	Charging and Remissions Policy	Financial Regulations	Retained until the date the policy is superseded + 3 years thereafter	SECURE DISPOSAL
i.	Independent auditor's reports	Financial Regulations	Retained for the financial year reports relate to + 6 years thereafter	SECURE DISPOSAL
j.	Funding Agreements	Financial Regulations	Retained for 6 years following the most recent payment	SECURE DISPOSAL
k.	Funding records – capital grant	Financial Regulations	Date of last payment of funding, plus six years	SECURE DISPOSAL
l.	Funding records – general annual grant	Financial Regulations	Date of last payment of funding, plus six years	SECURE DISPOSAL
m.	Per-pupil funding records	Financial Regulations	Date of last payment of funding, plus six years	SECURE DISPOSAL
n.	Exclusions agreements	Financial Regulations	Date of last payment of funding, plus six years	SECURE DISPOSAL
o.	Funding records	Financial Regulations	Date of last payment of funding, plus six years	SECURE DISPOSAL
p.	Gift aid and tax relief	Financial Regulations	Date of last payment of funding, plus six years	SECURE DISPOSAL
q.	Records relating to loans	Financial Regulations	Date of last payment of loan, plus six years if the loan is under £10,000 or date of last payment of loan, plus 12 years if the loan is over £10,000	SECURE DISPOSAL

Administrative Records

The table below outlines the Trust's retention periods for any other records and the action that will be taken after the retention period, in line with any requirements. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Administrative Information				
1. Operational Administration				
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	General file series		Retained for 5 years after the current academic year, and then reviewed	Review whether a further retention period is required and then SECURE DISPOSAL
b.	School brochure or prospectus		Retained for 3 years after the current academic year	STANDARD DISPOSAL
c.	Circulars (Staff/parents/pupils)		Retained for 1 year after the current academic year	STANDARD DISPOSAL
d.	Newsletters and other short-term documents		Retained for 1 year after the current academic year	STANDARD DISPOSAL
e.	Visitors' books/Signing in Sheets		Retained for 6 years after the current academic year, and then reviewed	SECURE DISPOSAL
f.	PTA/Alumni Associations		Retained for 6 years after the current academic year, and then reviewed	Review whether a further retention period is required and then SECURE DISPOSAL
g.	Privacy notices		Until superseded, plus six years	SECURE DISPOSAL
h.	Browsing data / cookies		15 months from the date of collection	STANDARD DISPOSAL
2. Local Authority (LA)				

	Basic File Description	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
a.	Attendance returns		Current year + 1 year	SECURE DISPOSAL
b.	Circulars from LEA		Whilst required operationally	SECURE DISPOSAL
c.	School census returns		Current year + 5 years	SECURE DISPOSAL
3.	**Department for Children, Schools and Families**			
	Basic File Description	**Statutory Provisions**	**Retention Period**	**Action at the end of the administrative life of the record**
a.	OFSTED reports and papers	N/A - Ofsted reports are publicly accessible and supplementary evidence is retained for 6 years should a complaint be raised	Reports to be retained until superseded by a more recent full inspection report	SECURE DISPOSAL
b.	Returns		Current academic year + 6 years	SECURE DISPOSAL
c.	Circulars from the Department for Children, Schools and Families		Whilst operationally required	SECURE DISPOSAL

Appendix B - Nominated GDPR Representatives

Data Protection (UK GDPR) Policy		
The names of and contact details for a nominated representative in each school/academy:		
Establishment	**GDPR Nominated Representative**	**Telephone Number**
Heartwood Learning Trust	Wendy Munro (COO, DPO) Lauren Oakes (Compliance Officer)	01904 560053
Liberty Academy	Glen Groizard	01482 781912
Aspire Academy	Nikola Crane	01482 318789
Barlby High School	Warren Carrington	01757 706161
The Compass Academy	Donna Murray	01482 331720
George Pindar School	Mark Ward	01723 582194
Graham School	Mark Ward	01723 366451
Manor CE Academy	Rachael McNair	01904 798722
Vale of York Academy	Stacey Stump	01904 560000
Burton Green Primary School	Stacey Stump	01904 552380
Forest of Galtres Anglican Methodist Primary School	Rachael McNair	01904 470272
Newland St John's CE Academy	Connie Havercroft	01482 305740
Poppleton Ousebank Primary School	Gemma Stainer	01904 795930
Skelton Primary School	Dawn Chaplin	01904 555170
St James' CE Academy	Kerrie Todd	01482 825091