HOLLINGWORTH LEARNING TRUST
DATA PROTECTION POLICY

Reviewed:	Spring 2024
Version:	6
Next Review:	**Live Document:** To be updated as and when new advice and guidance is received regarding Data Protection, GDPR and Freedom of Information.
Review Body:	**To be reviewed by Trustees annually.**

VERSION INFORMATION

Version	Reason for Update	Author	Date	Approved By:
1	Original Policy	S Collinge J Hawkrigg	Summer 2014	Governors Estates Committee
2	Updated in line with legislation changes, GDPR and Data Protection Act 2018.	S Collinge	Spring 2019	Governors
3	Updated in line with changes to legislation and movement to a Multi Academy Trust – Hollingworth Learning Trust	S Collinge	Spring 2021	Trustees
4	Review and Update Amended Educational Record Requests.	S Collinge	Spring 2022	Trustees
5	Reviewed and Updated • Page 13 – Children and Subject Access Request, changed wording from Children under 12 to Children aged 13. • Page 21 – Linked to other policies • BYOD Policy removed from the list as no longer used. • Trust address updated within the document.	S Collinge	Spring 2023	Trustees
6.	Reviewed and Updated: • Wording Updated in Sections: 7.3, 7.7, 7.8, 10, 10.2, 11.1, 13, 14 & 15 • Section 8.2 – addition of Primary Schools • Section 12 – addition of Artificial Intelligence	S Collinge	Spring 2024	Trustees

CONTENTS

DATA AT HOLLINGWORTH LEARNING TRUST

1. AIM:

Hollingworth Learning Trust (HLT/the Trust) aims to ensure that all personal data collected about staff, pupils, parents/carers, governors, trustees, visitors and other individuals is collected, stored and processed in accordance with UK Data Protection Law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

The aim of this document is to set guidelines to enable staff, parents/carers and pupils to understand the processes and procedures in the following areas:

1. **The Data Protection Act**
2. **Right of Access**
3. **Biometric System**
4. **Digital Images**
5. **Records Management**

In order to operate efficiently, HLT has to collect and use information about the people with whom it works. These will include staff, pupils and parents/carers. In addition, it is required by law to collect and use information in order to comply with the requirements of Central Government.

2. SCOPE:

This policy applies to all pupils, employees, governors, trustees, contractors, agents and representatives and temporary staff working for or on behalf of the Trust.

This policy applies to all personal information created or held by the Trust and its academies in whatever format, (e.g. paper, electronic, email, microfiche, digital images) and however it is stored, (for example ICT system/database, shared drive filing structure, email, filing cabinet, shelving, and personal filing drawers).

3. LEGISLATION:

This policy meets the requirements of the UK General Data Protection Regulations (UK GDPR) and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with our Funding Agreement and Articles of Association.

It is a requirement of Trust schools that they comply fully with the current guidelines published by the RPA cyber security insurance and the National Cyber Security Centre Cyber Security for Schools available at Cyber Security for Schools - NCSC.GOV.UK**.**

4. DEFINITIONS

Term	Definition
Personal Data	Any information relating to an identified, or identifiable individual. This may include the individual's: • Name (including initials). • Identification number. • Location data. • Online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.
Special Categories of Data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin. • Political opinions. • Religious or philosophical beliefs. • Trade union membership. • Genetics. • Biometrics (such as fingerprints, retina, and iris patterns), where used for identification purposes. • Health – physical or mental. • Sex life or sexual orientation.
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. THE DATA CONTROLLER:

HLT processes personal data relating to pupils, parents, staff, governors, trustees, visitors, and others and, therefore, is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

6. ROLES AND RESPONSIBILITIES

This policy applies to all staff employed by HLT, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

6.1 The Trustees

The Board of Trustees has overall responsibility for ensuring that our Trust complies with relevant data protection obligations.

6.2 Headteacher

The Headteacher at each academy acts as the representative of the data controller on a day-to-day basis.

6.3 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the Trust's compliance with UK data protection law, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to the Board their advice and recommendation on Trust data protection issues.

The DPO is the first point of contact for individuals whose data the Trust processes, and for the ICO.

The trust DPO is Susan Collinge and is contactable at on 01706 292828 or via email at dpo@hltrust.co.uk.

6.4 All Staff

Staff are responsible:

- For collecting, storing, and processing any personal data in accordance with this policy.
- For informing the Trust of any changes to their personal data, such as change of address.
- For contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
  - If they have any concerns that this policy is not being followed.
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
  - If they need to rely on or capture consent, draft a privacy notice; deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
  - If there has been a data breach.
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
  - If they need help with any contracts or sharing personal data with third parties.

7. DATA PROTECTION

7.1 Personal Data

The UK GDPR defines personal data as:
"Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as: a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Personal data is information that relates to a living individual. That individual must be identified, or identifiable either directly or indirectly, from one or more identifiers or from factors specific to the individual.

The UK GDPR covers the processing of personal data in two ways:

- Personal data processed wholly or partly by automated means (that is, information in electronic form).
- Personal data processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is, manual information in a filing system).

7.2 Data Protection Principles

The UK General Data Protection Regulations are based on data protection principles that HLT must comply with.

The principles require that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how Hollingworth Learning Trust aims to comply with these principles.

7.3 Collection and Processing of Personal Data

HLT will only collect and process personal data where we have one of the six 'lawful bases' (legal reasons) to do so under data protection law:

1. **Contract**
   The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract.
2. **Legal Obligation**
   The data needs to be processed so that the Trust can **comply with a legal obligation**.
3. **Vital Interest**
   The data needs to be processed to ensure the **vital interests** of the individual, i.e. to protect someone's life.
4. **Public Interest**
   The data needs to be processed so that the Trust, as a public authority, can **perform a task in the public interest or exercise its official authority.**
5. **Legitimate Interest**
   The data needs to be processed for the **legitimate interests** of the Trust (where the processing is not for any tasks the Trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.

6. **Consent**
   The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

For special categories of personal data, the Trust must also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent.**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security, or social protection law.**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for the establishment, exercise or defence of **legal claims**.
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**.
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever the Trust initially collects personal data directly from individuals, we will provide them with the relevant information required by data protection law.
The Trust will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

7.4 Management of Data

The Trust is responsible for making sure that personal data is managed in accordance with the Data Protection Act. The Headteacher will act as the representative of the data controller for their academy on a day-to-day basis. All staff are responsible for ensuring that they read this policy and comply with it and the General Data Protection Regulation and Data Protection Act 2018. Where a member of staff has particular responsibility for data compliance, they should make sure they understand their role. **Staff are made aware that knowingly or recklessly disclosing personal data may be a criminal offence and that internal disciplinary procedures will be followed if a member of staff commits a data breach.**

7.5 Data Protection by Design and Default

The Trust will put measures in place to show that the Trust have integrated data protection into all of its data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 7).
- Completing data protection impact assessments where the Trust or academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws will apply.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

7.6 Limitation, Minimisation and Accuracy

- HLT will only collect data for specified, explicit, and legitimate reasons. When the Trust collects personal data directly from individuals, they will be provided with the relevant information required by data protection law.
- Under data protection law, individuals have a right to be informed about how the Trust uses any personal data that is held about them. The Trust will comply with this right by providing 'privacy notices' to individuals where the Trust is processing their personal data.

For a full list and copies of the Trusts Privacy Notices please see Appendix 1.
Copies of all the Trust privacy notices are available on the Trust's website.

- The Trust will always consider the fairness of data processing. The Trust will ensure that it does not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.
- If the Trust would like to use personal data for reasons other than those given when it was first obtained, the Trust will inform the individuals concerned before it does so and seek consent where necessary.
- Staff must only process personal data where it is necessary in order to do their jobs.
- The Trust will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.
- In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's Records Management Policy.

7.7 Data Security and Storage of Records

HLT will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper based records are kept in lockable filing cabinets.
- Portable electronic devices, such as laptops that contain personal data, are encrypted and can be remotely deleted.
- Papers containing personal data must not be left on office or classroom desks, on staffroom tables,

pinned to notice/display boards, or left where there is general public access.
- Staff are advised not to access personal data off-site, and if they do so, they are requested to use the academy's computer system, so security is in place to protect it. Paper copies should not be removed from site, where paper copies are removed, they should be kept in folders with the staff member's contact details.
- When taking information offsite, staff are informed that they must not leave paper documents or laptops in their cars. **Staff are responsible for keeping any information they access or remove from site secure.**
- As part of the Trusts 'Acceptable Use Policy' and 'Data Protection – Staff Guidance', staff must practice good IT security. This includes using strong passwords to access academy computers, laptops, and school systems and using encryption and passwords to protect documents. Staff should not reuse passwords used on other systems.
- Encryption software is used to protect all portable devices, such as laptops.
- Multi-factor authentication will be activated and must be used by staff on systems where it is available.
- Staff must not use USB sticks or hard drives.
- Staff, pupils, or governors who store personal information on their personal devices are expected follow the same security procedures as for trust-owned equipment (see BYOD Policy).
- Where the Trust needs to share personal data with a third party, the Trust will carry out the necessary due diligence and take reasonable steps to ensure it is stored securely and adequately protected.
- All staff are required to read and sign the 'Acceptable Use Policy' on an annual basis.

7.8 Sharing Personal Data

HLT will not normally share personal data with other organisations, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:
- There is a lawful basis to do so under data protection law.
- There is an issue with a pupil or parent/carer that puts the safety of pupils and staff at risk.
- When the Trust needs to liaise with other agencies – depending on the lawful basis, the Trust may request consent as necessary before doing this.
- When the Trust suppliers or contractors need data to enable the Trust to provide services to pupils and staff, for example IT companies. When doing so, the Trust will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law.
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep data safe whilst working with the Trust.

HLT will also share personal data with law enforcement and government bodies where the Trust is legally required to do so, including:
- The prevention or detection of crime/fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy the Trusts safeguarding obligations.
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

HLT may also share personal data with emergency services and local authorities to help them respond to an emergency that affects any of the Trust's pupils or staff.

Where the Trust transfers personal data internationally, it will do so in accordance with UK data protection law.

8. SUBJECT ACCESS REQUESTS

Individuals have a right to make a 'Subject Access Request (SAR or DSAR)' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this is not possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure, or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- The safeguards provided if the data is being transferred internationally.

8.1 How to make a Subject Access Request

Subject Access Requests can be submitted in any form, the Trust may be able to respond to requests more efficiently if they are made in writing and include:

- Name of the individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

If staff receive a Subject Access Request in any form, they must immediately forward it to the DPO.
A template of the Subject Access Request form can be found in Appendix 2

8.2 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent/carer to make a SAR with respect to their child, the child must either be unable to understand their rights and the implications of a SAR, or have given their consent.

- Primary School Pupils:
  Children aged 12 and below/under are generally not regarded to be mature enough to understand their rights and the implications of a Subject Access Request. Therefore, most Subject Access Requests from parents or carers of pupils who are aged 12 or under, may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

- Secondary School Pupils:
  Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SAR requests from parents/carers of a pupil at Hollingworth may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

8.3 Responding to Subject Access Requests

When responding to SARs the Trust may:

- Ask the individual to provide identification.
- Contact the individual via phone to confirm the request was made and clarify any queries.
- Will respond without delay within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant).

- The Trust must provide the SAR for free.
- Where a request is complex or numerous the Trust will comply within three months of the request. The Trust will inform the individual of this within one month and explain why the extension is necessary.

The Trust will not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the pupil is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the pupil's best interests.
- Would include another person's personal data that we can't reasonably anonymise, we don't have the other person's consent, and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.
When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

8.4 Subject Access Requests Submitted over school holidays

Individuals are entitled to submit a SAR all year round. However, it may be necessary for the Trust to extend the response period when requests are submitted during school holidays. This is in accordance with article 12(3) of the GDPR and will be the case where the request is complex, e.g. where the Trust needs multiple staff to deal with the request.

8.5 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request, and to receive information when the Trust is collecting an individual's data about how the Trust will use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask the Trust to rectify, erase or restrict processing of their personal data (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement).
- Be notified of a data breach (in certain circumstances).
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

9. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

In all maintained schools, pupil referral units and non-maintained special schools, parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil).

In academies, there is no equivalent right of access. To support parental engagement, our academies offer 'Parent Access' to their Management Information Systems which enables parents/carers to view information about their child's education record. Parents/carers should use this application before submitting a request to view their child's educational record.

Parents must submit a Subject Access Request to view their child's educational record. Please see the section on Subject Access Requests for further information.

10. BIOMETRIC RECOGNITION SYSTEMS

Biometric data is physical characteristics or biological measurements that can be used to identify individuals. At HLT, where we use pupils' biometric data as part of an automated biometric recognition system, for example, pupils use fingerprints to receive school dinners instead of paying with cash, we will comply with the requirements of the Data Protection Act and Protection of Freedoms Act 2012 in the way we collect and handle biometric information.

10.1 Notification

Parent/carers will be notified before any biometric recognition system is put in place or before their child takes part in it. All parents/carers are notified when their child joins the Trust and details are included in the admissions information. The Trust will request written consent from the parent/carer as part of the admissions process.

10.2 Consent

Parents/carers and pupils have the right to choose whether to use the academy's biometric system. The academy will provide alternative means of accessing the relevant services for those pupils who choose not to use the systems. Parents/carers and pupils can withdraw consent at any time. When consent is withdrawn, the academy will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, the academy will not process that data irrespective of any consent given by the pupil's parent/carer.

10.3 Trust Staff

Where staff members or other adults use the academy's biometric systems, the academy will also obtain their consent before they first take part in it, and provide an alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the academy will delete any relevant data already captured.

11. DIGITAL IMAGERY GUIDANCE

(During this guidance, where the Trust refers to 'Photography' this will also include reference to Digital Imagery and Filming).

As part of our Trust's activities, we may take photographs and digital images of individuals.

11.1 Notification & Consent

HLT Academies will obtain written consent from parents/carers, for photographs and digital images to be taken of pupils for communication, marketing, and promotional materials. Parents/carers will be notified about digital imagery procedures in the Trust when their child joins their academy and details are included in the admission information. This information explains how digital images will be used. The Trust will request written consent from the parent/carer as part of the admissions process.

11.2 Digital Imagery Use

Our Academies may use digital images, video footage or audio recordings of individuals during their time at school. These images, footage or recordings may be used in:

- Internal academy displays.
- The Trust and academies' website or social media.
- The academy prospectus.
- The Trust and academies' newsletter or other promotional materials.

They may also:

- Be made publicly available in the media, including print copies.
- Be made available to the national press, other news or industry media (both print and web).

Consent can be refused or withdrawn at any time. If consent is withdrawn, the Trust will delete the photograph or video and not distribute it further.

When using digital images in this way the Trust will not accompany them with any other personal information about the child, to ensure they cannot be identified. Parents/carers and pupils are made aware that once a photograph or video appears in the media, the Trust have no control over who else may use or view the images, or how long the images remain available to use or view.

11.3 Digital Imagery & Examinations

As part of many courses, it is a requirement of the examination board that digital images, video evidence or audio recordings are provided to demonstrate pupils' ability and although associated risks are minimal, educational establishments have a duty of care towards pupils. HLT recognises the need to ensure the welfare and safety of all young people.

The images, footage and recordings taken will be securely stored on the academy's servers, along with a copy of the consent form. Only Trust staff will have access to the stored copies of the files. The images, footage and recordings taken are securely disposed of once any appeals/validation processes have been completed.

11.4 Family Photographs at Academy Events

Any photographs and videos taken by parents/carers at academy events are for their own personal use are not covered by data protection legislation.

- It shall be at the discretion of the academy whether photographs may be taken at an academy event.
- The Data Protection Act will not cover family taking photographs for the family album.
- Where the academy decides to allow such photography, the parents/carers will be asked not to share the digital images publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

11.5 Trust Staff
Where digital images of staff members or other adults are used, the Trust will obtain their consent.

Staff and other adults can also withdraw consent at any time, and the academy will delete any relevant data already captured.

11.6 Storage & Retention
The images, footage and recordings taken will be securely stored by the academy. Consent forms will be stored on staff and pupil's files. Only Trust staff will have access to the stored copies of the files.

The Trust takes all the necessary steps to ensure that any images produced are used solely for the purposes for which they are intended. The images will never be sold or used for purposes other than those stated above.

In some cases, digital images, video footage and audio recordings may be stored and used after an individual has left the Trust and will continue to do so until updated. Parents/carers, pupils and staff are informed that digital Images may be used up to two years after an individual has left the Trust.

12. ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.
Hollingworth Learning Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.
To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots. If personal and/or sensitive data is entered into an unauthorised generative AI tool, HLT will treat this as a data breach and will follow the personal data breach procedure outlined in Appendix 3.

13. RECORDS MANAGEMENT

Hollingworth Learning Trust recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the Trust. Records provide evidence for protecting the legal rights and interests of the Trust and provide evidence for demonstrating performance and accountability. For further information please see the Trust's Records Management Policy.

13.1 Retention of Records

Records will be retained or disposed of appropriately in accordance with the Trust's statutory obligations and having regard to the Retention Guidelines for schools published by the Information and Records Management Society. These guidelines can be found at:
http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school

13.2 Disposal of Records

Personal data and records that are no longer needed must be disposed of securely.
Personal data that has become inaccurate or out of date will also be disposed of securely, where the Trust cannot or do not need to rectify or update it.
Paper based records and confidential waste should be disposed of using the confidential waste provisions at each academy.

Electronic files will be deleted securely by IT.

14. 14. PERSONAL DATA BREACHES

A data breach occurs when data/information is lost, stolen or wrongfully disclosed If a data breach occurs there are steps that the Trust can take to reduce the impact of the breach. The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the Trust will follow the data breach procedure in Appendix 3.

All staff are informed that suspected data breaches must be reported to the Trust Data Protection Officer as soon as they are aware. A data breach must be reported by emailing the academy's IT Helpdesk and dpo@hltrust.co.uk.
When appropriate, the Trust will report the data breach to the ICO within 72 hours. Such breaches in an academy may include, but are not limited to:

- A non-anonymised dataset being published on the academy website that shows exams results of pupils eligible for pupil premium.
- Safeguarding information being made available to an unauthorized person.
- The theft of a laptop.

Further information and guidance are available in '*Data Protection – Staff Guidance*' which will be shared annually with staff.

15. TRAINING

All staff are provided with data protection training as part of their induction process.
This includes the following online courses:

- UK GDPR in Education – Every 2 years
- NCSC Cyber Security Training - Annually

Staff are also required to read on arrival at the Trust and annually thereafter:

- Staff Guidance document
- Data Protection on a Page

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

16. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed **annually** and approved by the Board of Trustees.

17. LINKS WITH OTHER POLICIES & GUIDANCE

- **Freedom of Information**
  For further information about how HLT meets it obligations of the Freedom of Information Act, please see the Trust Freedom of Information Policy & Freedom on Information Publication Scheme.
  The Trust Freedom of Information Publication Scheme is available on the Trust Website at:
  https://hltrust.co.uk/trust-policies-key-documents/policies
- **CCTV**
  HLT use CCTV on our academy sites to ensure it remains safe and secure. HLT will adhere to the ICO's code of practice for the use of CCTV. HLT does not need to ask individuals' permission to use CCTV, but each site will make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
  Any enquiries about the CCTV system should be directed to the DPO. For further information regarding CCTV please see the individual academy's CCTV Policy.

  The Trust CCTV Policy is available on the Trust Website at:
  https://hltrust.co.uk/trust-policies-key-documents/policies
- **Safeguarding**
  For further information about HLT meets its safeguarding obligations please see the Trusts Safeguarding policy available on each academy's website.
- **Trust Acceptable Use Policy**
- **Retentions Management Policy**
- **Staff Guidance Documents:**
  - Data Protection on a Page
  - Data Protection – Staff Guidance

APPENDICIES

1. Trust Privacy Notices
2. Subject Access Request Form
3. Personal Data Breach Procedure

Appendix 1: Trust Privacy Notices

The Trust has the following Privacy Notices:

- Pupil Privacy Notice
- Pupil Privacy Notice - 12 year +
- Parent & Carer Privacy Notice
- Staff Workforce Privacy Notice
- Governors Privacy Notice
- Recruitment Privacy Notice
- Visitors Privacy Notice
- Website Privacy Notice

All these are available on the Trust/academy website at:
https://hltrust.co.uk/trust-policies-key-documents/policies

A link to these notices will be available on each academy's website.

Appendix 2: Subject Access Request Form

This form is to be used when an individual submits a subject access request to Hollingworth Learning Trust.

For Staff:
Please see the Subject Access Request Procedure for more information. Please seek advice from the Trust's Legal Support if you have any queries or concerns regarding a SAR or SAR response.

Date:
Location (select one): Hollingworth Academy
Newhouse Academy
Hollingworth Learning Trust

Re: Subject Access Request

Please complete the following form to request information held about you at Hollingworth Learning Trust. To assist the Trust in completing your request please provide us with the information stated below. The Trust will cooperate with all requests, detailing the information that is processed and verifying the lawfulness of the processing.

Name:	
Relationship with the school:	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested:	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible.*

The Trust will contact you:

- To clarify/confirm information requested.
- To inform you of the expected time to process the request and if an extension is required (for complex requests).

If you have any questions, concerns or would like more information about anything mentioned in this letter, please contact our Data Protection Officer at dpo@hltrust.co.uk

For Office Use Only:

Date Received:	Received By:
Date sent to DPO:	Ref No:

Appendix 3: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor, trustee or data processor must immediately notify the data protection officer (DPO) and Trust IT by:
  - **Emailing the IT Helpdesk at your academy**
  - **Emailing the DPO at dpo@hltrust.co.uk**
  - **Or by telephone at 01706 292 805**.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been made available to unauthorised people.
- Staff, governors and trustees will cooperate with the investigation, including allowing access to information and responding to questions. The investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Headteacher and, if necessary, the Chair of Governors or Chair of Trustees.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required. (See the actions relevant to specific data types at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the DPO on the Trust's relevant GDPR system, currently GDPRiS. They are held for two years in line with ICO guidance.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the Trust's awareness of the breach. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible.
  - The categories and approximate number of individuals concerned.
  - The categories and approximate number of personal data records concerned.
  - The name and contact details of the DPO.
  - A description of the likely consequences of the personal data breach.
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the Trust's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

- Where the Trust is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach.
  - The name and contact details of the DPO.
  - A description of the likely consequences of the personal data breach.
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police or insurers.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause.
  - Effects.
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).
- Records of all breaches will be stored by the DPO.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- The DPO and Headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the Trust/academy to reduce risks of future breaches.

Actions to minimise the impact of data breaches

Below are data breach scenarios and the steps the Trust may take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. The Trust will review the effectiveness of these actions and amend them as necessary after any data breach.

Scenario 1: Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [IT Department to attempt to recall it from external recipients and remove it from the Trust/academy's email system (retaining a copy if required as evidence).
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it is appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the trust/academy should inform it safeguarding partners.

-

Scenario 2: A staff laptop, device or paper documentation is lost or stolen

- Staff are responsible for any trust/academy devices or paper records they take from site. These should not be left in vehicles overnight and should be stored securely in the home.
- If a laptop, paper documents or other trust/academy device is stolen, the member of staff should email their **IT Helpdesk and the Trust DPO at dpo@hltrust.co.uk** as soon as they are aware. If this happens in the evening or over a weekend, staff should email as soon as possible and not wait until they are next in school.
- All encrypted trust/academy devices can be remotely disabled, and will be done so by IT.
- If paper documents have been lost or stolen, the member of staff must inform the DPO of the documents lost, and if the documents contained any sensitive or personal information.

Scenario 3: A Staff laptop or device is hacked

- All staff must complete the NCSC Cyber Security Training annually.
- If staff believe their laptop or other Trust/academy device has been hacked, or they feel they have responded to a phishing email, the member of staff should email their **IT Helpdesk and the Trust DPO at dpo@hltrust.co.uk** as soon as they are aware. If this happens in the evening or over a weekend, staff should email as soon as possible and not wait until they are next in school.
- All encrypted trust/academy devices can be remotely disabled, and will be done so by IT.