Data Protection Policy

LIGHTHOUSE
MULTI ACADEMY TRUST

Policy Owner:	Lighthouse Multi Academy trust
Approved/ Ratified:	Pat Hunt
Review Dates:	July 2027

Document Version Control Log

Version	Modification Date	Synopsis of Changes
1.0	September 2025	
2.0	June 2025	Section 2: updated legislation Section 11: Updated CCTV as each academy has their own policy due to being bespoke sites Section 12: Social media and photo/ video permission section updated Section 13: Added further DfE recommended guidance regarding AI Updated Policy list to read in conjunction with this policy

Contents

1. Aims

Our Lighthouse Multi Academy Trust aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, 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.

2. Legislation and guidance

This policy has been developed in accordance with the following legislation, statutory requirements and recognised guidance:

Legislation

- **UK General Data Protection Regulation (UK GDPR),** as incorporated into UK law following the UK's withdrawal from the European Union.
- **Data Protection Act 2018 (DPA 2018)**.
- **Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR),** where applicable.
- **Freedom of Information Act 2000 (FOIA)**.
- **Environmental Information Regulations 2004 (EIR),** where applicable.
- **Human Rights Act 1998,** particularly Article 8 – the right to respect for private and family life.
- **Education Acts** and other relevant legislation relating to the processing of personal information within educational settings.

Department for Education and Government Guidance

This policy reflects guidance published by:

- Department for Education (DfE) **Cyber Security Standards for Schools and Colleges**.
- Department for Education guidance on **Generative Artificial Intelligence in Education**.
- National Cyber Security Centre (NCSC) guidance on cyber security and information assurance for schools and trusts.

Information Commissioner's Office (ICO) Guidance

This policy is informed by guidance published by the Information Commissioner's Office (ICO), including:

- **ICO Accountability Framework**.
- **Guide to the UK GDPR**.
- **Data Protection Act 2018 Guidance**.
- **Children's Code (Age Appropriate Design Code),** where relevant to online services used by children.
- Guidance on **CCTV and Surveillance Cameras**.
- Guidance relating to artificial intelligence, biometric data, records management, data sharing and information security.

Information and Records Management

The Trust also has regard to:

- **Information and Records Management Society (IRMS) Schools Toolkit,** including records retention guidance and best practice for information governance.

Trust Compliance

This policy also supports compliance with the Trust's:

- Funding Agreement.
- Articles of Association.
- Records Management and Retention Schedule.
- Information Security, Cyber Security and Acceptable Use Policies.
- Freedom of Information Publication Scheme and associated policies.

The Trust is committed to ensuring that all personal data is processed lawfully, fairly and transparently, and that appropriate technical and organisational measures are in place to protect personal information in accordance with data protection legislation and recognised best practice.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living 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 personal 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 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.

4. The data controller

Our Academy processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Academy is registered with the ICO / has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

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

5.1 The Trustees/ Governors/ Governing board

The Lighthouse Multi Academy Trust has overall responsibility for ensuring that the academies and Trust comply with all relevant data protection obligations.

Trustees receive assurance regarding data protection compliance through reports from the Trust DPO and Trust Central Team, including significant breaches, trends and compliance monitoring.

5.2 Trust Central Team

All academies will notify the Trust Central Team termly of any data breaches which will be reported to the Trust board on a termly basis.

Each academy will have a nominated GDPR lead at a local level to ensure that a strong data protection culture is established across the Trust. This nominated lead will liaise regularly with the Trust Central Team regarding any data breaches.

Half termly the Trust Central Team will view each academy's Data Breach Register (Appendix 2) and provide actions or training as appropriate.

5.3 Trust Data protection officer (DPO)

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

They will provide an annual report of their activities directly to the trustees/ governing board and, where relevant, report to the trustees/ board their advice and recommendations on academy data protection issues.

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

Full details of the Trust DPO's responsibilities are set out in their job description.

The Data Protection Officer is presently Walsall Council. Each academy will have a designated member of staff responsible for data protection and liaise with the DPO as required.

5.4 Headteacher

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

5.5 Nominated GDPR Lead

Each academy will have a nominated GDPR lead who will internally lead data protection and complete Appendix 2 Data Breach register to track any level data breaches.

The data breach register will be shared with the Trust Central team half termly and analysed data will be presented to the Trustees termly.

The GDPR Lead should:

- maintain the Record of Processing Activities (ROPA)
- coordinate DPIAs
- monitor compliance with privacy notices
- support information governance audits

5.6 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Academy of any changes to their personal data, such as a change of address
- Contacting the Trust 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

6. Data protection principles

The UK GDPR is based on data protection principles that our Academy must comply with.

The principles say 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 the Academy aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Academy can **fulfil a contract** with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the Academy, as a public authority, can **perform a task in the public interest or exercise its official authority**

- The data needs to be processed for the **legitimate interests** of the Academy (where the processing is not for any tasks the Academy performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- 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, we will also meet 1 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 we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We 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.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We 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 Academy's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

International transfers will only take place where appropriate safeguards are in place under UK GDPR.

Where appropriate, formal Data Sharing Agreements will be established with partner organisations.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy 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 isn't 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

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address

- Contact number and email address
- Details of the information requested

Requests may be submitted electronically, verbally or in writing.

If staff receive a subject access request in any form they must immediately forward it to the DPO and notify the Trust Central Team. e.g The Director of Safeguarding and Attendance

9.2 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 or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 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 at our Academy 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.

Children aged 12 and above are generally 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 at our Academy 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.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may 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 child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and 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.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time

- Ask us 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 that 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.

10. Parental requests to see the educational record

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) within 15 Academy days of receipt of a written request.

If the request is for a copy of the educational record, the Academy may charge a fee to cover the cost of supplying it. Each Academy will charge 20p per black and white copy per page and a charge in line with current post office charges.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

Individual academies within the Trust may operate CCTV systems on their sites to help maintain a safe and secure environment for pupils, staff, visitors and property.

Each academy's CCTV arrangements are detailed within its own CCTV policy, which can be found on the academy's website. All academies follow the guidance issued by the Information Commissioner's Office (ICO's guidance) and comply with relevant data protection legislation and principles.

Where CCTV is in operation, cameras will be clearly visible and appropriate signage will be displayed to inform individuals that recording is taking place. Consent is not required for the use of CCTV where it is being used for legitimate purposes such as safety and security; however, academies will ensure that its use remains lawful, fair and proportionate.

Any enquiries regarding an academy's CCTV system should, in the first instance, be directed to the individual academy. If further support is required, enquiries may then be escalated to the Trust Central Team.

12. Photographs and videos

The academy may take photographs and videos of pupils during school activities and events. These images may be used for educational purposes, displays, newsletters, the academy website, and social media.

Under the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, the academy will obtain parental permission before using photographs or videos of children.

We will obtain **written consent** from parents/carers giving them choices to opt in or out of photographs and videos in different contexts. This consent form is sent as part of the admissions paperwork and must be completed by a parent/ carer with parental responsibility. (PR)

Where the Trust/Academy takes photographs and videos, uses may include:

- **Educational purposes** — including assessment, learning support, and classroom activities (e.g. performing music, presentations, speaking in lessons, Tapestry, and learning journeys/ pupil books).
- **Internal displays** — within classrooms and around the academy.
- **Academy and Lighthouse Multi Academy Trust website**.
- **Electronic newsletters** — in the weekly academy newsletter and the half-termly Lighthouse Multi Academy Trust newsletter shared electronically with parents and carers.
- **Academy prospectus** — shared in paper format with prospective parents and carers
- Outside of Academy by external agencies such as the Academy photographer, newspapers, campaigns

The Academy and Lighthouse Multi Academy Trust may share photographs and videos of pupils on official social media accounts, including Facebook, Instagram, TikTok, X (formerly Twitter), and LinkedIn.
Please note:
- Parents and carers have the right to withdraw consent at any time.
- Requests to withdraw consent must be made in writing.
- The academy will stop using images in future posts once consent is withdrawn.
- The Trust will consider requests for removal on a case-by-case basis, particularly where safeguarding, welfare or legal considerations apply.
- The academy cannot guarantee removal of content that has already been shared, copied, or downloaded by third parties.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Any photographs and videos taken by parents/carers at Academy events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

For more information on our use of photographs and videos see the following policies:

- Academy Safeguarding policy and child protection
- Trust Social Media
- Trust Admissions Policy

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with suitable AI agents which are risk assessed before use. The Lighthouse Academy 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, The Lighthouse Academy Trust will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

Staff must not upload confidential, personal or safeguarding information into publicly available generative AI tools unless the Trust has approved the platform, completed the necessary data protection checks and confirmed that appropriate contractual and security safeguards are in place.

All AI systems used within the Trust and its academies will undergo an appropriate Data Protection Impact Assessment (DPIA) where required prior to implementation.

Staff remain responsible for all decisions made using AI-assisted outputs and must check information for accuracy before use.

For more information, please read the Trust Artificial Intelligence Policy.

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our 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 6)
- Completing data protection impact assessments where the 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 may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Academy and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - The Trust publishes privacy notices for pupils, parents, staff, governors, volunteers, contractors and visitors on the Trust and academy websites.
    - 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

15. Data security and storage of records

We 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 and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the Academy office
- Passwords that are at least 10 characters long containing letters and numbers are used to access Academy computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Where available, multi-factor authentication (MFA) will be enabled for systems processing personal or sensitive information.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices/ hard drive devices
- Personal devices used to access Trust systems must comply with the Trust's acceptable use, encryption and security requirements.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Academy-owned equipment (see our online safety policy and acceptable use agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

The Trust will follow the Department for Education Cyber Security Standards for Schools and Colleges and ensure appropriate technical and organisational measures are in place to protect personal information from cyber threats.

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Records will be retained and disposed of in accordance with the Trust Records Retention Schedule and the Information and Records Management Society (IRMS) Toolkit for Schools where applicable.

17. Personal data breaches

The Academy will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

The designated person responsible in each academy will notify the Trust DPO of any data breaches. The Trust DPO will notify The CEO/ Trust Central Team of any academy breaches, who will then make arrangements to inform the Trustees.

All academies will notify the Trust Central Team/ CEO termly of any data breaches which will be reported to the Trust board on a termly basis.

Each academy will have a nominated GDPR lead at a local level to ensure that a strong data protection culture is established across the Trust. This nominated lead will liaise regularly with the Trust Central Team regarding any data breaches.

Half termly the Trust Central Team will view each academies Data Breach Register (Appendix 2) and provide actions or training as appropriate.

Serious breaches will be reported immediately to the Trust DPO and relevant senior leaders and not held until the termly reporting cycle.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in an Academy context may include, but are not limited to:

- A non-anonymised dataset being published on the Academy website, which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of an Academy laptop containing non-encrypted personal data about pupils

18. Training

All staff and governors are provided with data protection training as part of their academy induction process.

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

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the Trustees and full governing board.

20. Links with other policies

This data protection policy is linked to our:

- Academy Safeguarding and Child Protection Policy
- Academy CCTV Policy
- Academy GDPR Policy
- Trust Freedom of information Policy
- Trust Privacy notices
- Trust Mobile Phone Policy
- Trust Artificial Intelligence Policy
- Trust Online Safety Policy
- Trust Information Technology Policy
- Trust Records Management Policy
- Trust Social Media Policy
- Trust Admissions Policy
- Trust Cyber Security Policy

Appendix 1: 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 or data processor must immediately notify the Data Protection Officer (DPO) by email or phone.
- The Trust 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 and governors will co-operate 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 Trust DPO will alert the Headteacher and the chair of governors
- The Trust DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the Trust DPO with this where necessary, and the Trust DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The Trust 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 Trust 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 Trust DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in a secure location.
- Where the ICO must be notified, the Trust 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 Academy'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 Trust 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 Trust DPO will report as much as they can within 72 hours of the Academy's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the Trust DPO expects to have further information. The Trust DPO will submit the remaining information as soon as possible

Appendix 2 Data Breach Register

Under the GDPR each academy within the Lighthouse Multi Academy Trust is required to keep a record of all personal data breaches even if the breach does not meet the threshold to be reported to the ICO. The table below will be used as a basis for each academy within the Lighthouse Multi Academy Trust. This register must be kept highly confidential and only be accessed by those staff who need to use it. Please note that the ICO may request to see this register to check that the academy and Lighthouse Multi Academy Trust are complying with its obligations under the GDPR.

Date of breach	Risk rating	Outline of facts	Effect of the breach	Remedial action taken	Informed/ advice gathered from the Trust Central Team	ICO reportable? Yes/ No