Data Protection Policy (LLT)

LYDIATE LEARNING TRUST

ENGAGE, ENABLE, EMPOWER

Origination	*Authorised by*	*Policy Date*	*Review Date*	
JDA	***LLTBoard***	***Jan 26***	***Jan 29***	*Page 1 of 14*

Data Protection Policy (LLT)

Contents

..... 1

Contents 1

1. Aims 3

2. Legislation and Guidance 3

3. Definitions 3

4. The Data Controller 4

5. Roles and Responsibilities 4

6. Data Protection Principles 5

7. Collecting Personal Data 6

8. Sharing Personal Data 9

9. Subject Access Requests and Other Rights of Individuals 10

10. Parental Requests to see the Educational Record 12

11. Biometric Recognition Systems 13

12. CCTV 13

13. Photographs and Videos 13

14. Data Protection by Design and Default 14

15. Data Security and Storage of Records 15

16. Disposal of Records 16

17. Personal Data Breaches 16

18. Training 17

19. Monitoring Arrangements 17

20. Links with Other Policies 17

21. Document Version Control Log 19

Data Protection Policy (LLT)

1. Aims

Lydiate Learning Trust (The Trust) aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

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

2. Legislation and Guidance

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. 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 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 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.

4. The Data Controller

The Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The Trust is joint controller with the schools within the Trust of which Lydiate Learning Trust acts as multi-academy trust and parent company.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. The Trust schools are registered under the same ICO registration – Registration number Z2903637.

5. Roles and Responsibilities

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

5.1 Trust Board

The Trust board has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

5.2 Data Protection Officer

The 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 governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust and its schools process, and for the ICO.

The Trust schools all share the same DPO as joint controllers with the Trust.

Full details of the DPO's responsibilities are set out in their SLA.

Our DPO is SchoolPro TLC Limited and is contactable: **Tel**: 01452 947633
Email:contact@schoolpro.uk **Website** DPO@SchoolPro.uk

5.3 Executive Director of People and Culture

The Executive Director of People and Culture acts as the representative of the data controller on a day-to-day basis but may discharge this duty to a known and identified individual for the purposes of carrying out actions defined in this policy.

5.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the Trust of any changes to their personal data, such as a change of address.
- 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 European Economic Area.
    - 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 Trust 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 Trust 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 one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust and its schools can perform a **public task,** and carry out its official functions.
- The data needs to be processed so that the Trust and its schools can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the Trust and its schools can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
- The data needs to be processed for the **legitimate interests** of the Trust, its schools, or a third party (provided the individual's rights and freedoms are not overridden).
- Where the above does not apply we shall request clear **consent** from the individual (or their parent/carer when appropriate in the case of a pupil).

For further detail of which lawful basis is used for each category of data, see the relevant privacy notice.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018. This is laid out in more detail in point 7.3.

If we offer online services to pupils, such as classroom apps, we intend to rely on Public Task as a basis for processing, where this is not appropriate we will get parental consent for processing (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

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.

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 record retention schedule.

7.3 Our processing of special categories of personal data and criminal offence data

As part of our statutory functions, we process special category data and criminal offence data in accordance with the requirements of Articles 9 and 10 of the UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special Category Data

Special category data is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

Criminal Conviction Data

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Appropriate Policy Document

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This section of our Data Protection Policy document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notice and staff privacy notice.

Conditions for processing special category and criminal offence data

We process special categories of personal data under the following UK GDPR Articles:

i. Article 9(2)(a) – explicit consent

   In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

   Examples of our processing include staff dietary requirements and health information we receive from our pupils who require a reasonable adjustment to access our services.

ii. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Trust, its schools, or the data subject in connection with employment, social security or social protection.

   Examples of our processing include staff sickness absences.

iii. Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.

An example of our processing would be using health information about a pupil or member of staff in a medical emergency.

iv. Article 9(2)(f) – for the establishment, exercise or defence of legal claims.

Examples of our processing include processing relating to any employment tribunal or other litigation.

v. Article 9(2)(g) - reasons of substantial public interest.

As a Trust, we provide a safeguarding role to young and vulnerable people. Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role.

Examples of our processing include the information we seek or receive as part of investigating an allegation.

vi. Article 9(2)(j) – for archiving purposes in the public interest.

The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – archiving.

An example of our processing is the transfers we make to the County Archives as set out in our Records Management Policy.

We process criminal offence data under Article 10 of the UK GDPR

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Processing which requires an Appropriate Policy Document

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the APD for the Trust. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. Our retention with respect to this data is documented in our retention schedules.

Description of data processed

We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any union. Further information about this processing can be found in our staff privacy notice.

We process the special category data about the children in our care and other members of our community that is necessary to fulfil our obligations as a Trust, and for safeguarding and care. This includes information about their health and wellbeing, ethnicity, photographs and other categories of data relevant to the provision of care. Further information about this processing can be found in our pupil privacy notice.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Schedule 1 conditions for processing

Special category data

We process SC data for the following purposes in Part 1 of Schedule 1:

- Paragraph 1(1) employment, social security and social protection.

We process SC data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- Paragraph 6(1) and (2)(a) statutory, etc. purposes
- Paragraph 18(1) – safeguarding of children and of individuals at risk

Criminal offence data

We process criminal offence data for the following purposes in parts 1, 2 and 3 of Schedule 1:

- Paragraph 1 – employment, social security and social protection
- Paragraph 6(2)(a) – statutory, etc. purposes
- Paragraph 12(1) – regulatory requirements relating to unlawful acts and dishonesty etc
- Paragraph 18(1) – safeguarding of children and of individuals at risk
- Paragraph 36 – Extension of conditions in part 2 of this Schedule referring to substantial public interest

8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so 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 may seek consent if necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT and communication companies, education support companies, and those that provide tools for learning. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with 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 them safe while working with us

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

- The prevention or detection of crime and/or 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 our safeguarding obligations.
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

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.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

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 Trust or its schools hold 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.
- 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.

Subject access requests should be submitted in writing, either by letter, email or fax to the DPO. They should include:

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

If staff receive a subject access request, they must immediately forward it to SchoolPro contact@schoolpro.uk.

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, some subject access requests from parents or carers of pupils at our schools 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.

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.
- 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 will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

When responding to a Subject Access Request, we will carry out reasonable and proportionate searches to locate personal data. This means we will:

- Identify systems and records where relevant personal data is likely to be held.
- Avoid excessive or irrelevant searches that would place an undue burden on the organisation.
- Take into account the nature of the request, the context of the data, and the effort required to retrieve it.

This approach ensures we meet our obligations while balancing practicality and fairness.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

The UK GDPR does not prevent a data subject making a subject access request via a third party. Requests from third parties are dealt with as follows:

- In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the data subject.
- It is the third party's responsibility to provide evidence of this entitlement.
- This might be a written authority to make the request, or it might be a more general power of attorney.
- If there is no evidence that the third party is authorised to act on behalf of the data subject, we are not required to respond to the SAR.

- However, if we are able to contact the data subject, we will respond to them directly to confirm whether they wish to make a SAR.

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, where consent is the basis for processing.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).
- Prevent processing that is likely to cause damage or distress.
- 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 Executive Director of People and Culture or DPO. If staff receive such a request, they must immediately forward it to the DPO or People and Culture team.

Under Section 164A of the Data Protection Act 2018, you have a statutory right to complain if you believe your personal data has been handled inappropriately.

If you wish to raise a concern about how we process your personal data, please contact the People and Culture team or SchoolPro contact@schoolpro.uk . We will acknowledge your complaint within 30 days of receipt and take appropriate steps to investigate and respond without undue delay.

If you are not satisfied with our response, you may escalate your complaint to the Information Commission at: Information Commissioner's Office

It is important to note that the Trust and/or its schools could be reported to the Information Commissioner (ICO) for failing to comply with their statutory responsibilities regarding SARs and other data protection rights of the individual, and penalties (including financial) may apply.

10. Parental Requests to see the Educational Record

There is no equivalent legal right for parents, or those with parental responsibility to free access their child's educational record for a child that attends one of the schools within the Trust. It will be up to the Trust or school to decide whether to grant such access, and it is likely to depend on the contractual relationship between the parent and the school.

11. Biometric Recognition Systems

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

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 Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Trust or its schools will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the Trust or school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

Parents/carers and pupils can object to participation in the Trust or school's biometric recognition system(s), or withdraw consent, at any time, and we 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, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

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

12. CCTV

We use CCTV in various locations across the Trust's schools to ensure they remain safe. We will adhere to the ICO's guidance for the use of surveillance systems including CCTV.

We do not need to ask individuals' permission to use CCTV, but we 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 IT Manager.

13. Photographs and Videos

As part of our Trust and school activities, we may take photographs and record images of individuals within our Trust or its schools.

We will not seek consent from parents/carers for photographs and videos to be taken of their child for educational purposes for use in the classroom and school displays. We will process these images under the legal basis of Public Task.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within schools on public area notice boards and in school magazines, brochures, newsletters, etc.
- Outside of schools by external agencies such as the school photographer, newspapers, campaigns
- Online on our Trust and school websites or social media pages

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

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

See our CCTV Policy and Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

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 (DPIAs) where the Trust'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 – see section 14.1).
- 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, including:
    - Working with our appointed external audit partner, to conduct independent audits of data protection practices ever 3 years.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Trust and its schools, 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

14.1 Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project.

We will do a DPIA for processing that is **likely to result in a high risk** to individuals as well as any other major project which requires the processing of personal data.

It is vital that the **DPIA is completed before processing is commenced** to ensure that all risks are identified and mitigated as much as possible.

Our DPIA will:

- Describe the nature, scope, context, and purposes of the processing.
- Assess necessity, proportionality, and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

To assess the level of risk, we will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

We will consult our data protection officer (SchoolPro TLC Ltd) and, where appropriate, individuals and relevant experts. We may also need to consult with relevant processors.

If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing.

We will implement the measures we identified from the DPIA, and integrate them into our policies, procedures, and practice.

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, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must follow the relevant Trust and/or school procedures and ensure all records and copies are returned to the Trust or school.
- Passwords procedures should be followed as below:
    - Passwords used to access school computers, laptops, and other electronic devices should be at least 12 characters long and include a mix of uppercase and lowercase letters, numbers, and special characters. This increases the complexity of the password and makes it more difficult for unauthorized individuals to guess or crack.

  - Staff and pupils are advised not to change their passwords at regular intervals unless there is a suspected security breach. Instead, focus should be on creating a strong, unique password that is not easily guessable.
  - Remember not to share your passwords with anyone and avoid using personal information such as your name, date of birth, or common words as your password. Consider using a passphrase, which is a sentence-like string of words that is longer than a traditional password, easy to remember, and difficult to crack.
  - It's also recommended to use a reputable password manager to securely store and manage your passwords. This allows you to use unique, complex passwords for each service without the need to remember them all.

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust or school-owned equipment (see our Electronic Information and Communications Policy.
- 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).

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 Trust or school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal Data Breaches

The Trust and its schools 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 the Data Breach Policy.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in the Trust and its schools' context may include, but are not limited to:

- A non-anonymised dataset being published on the Trust or school/company websites which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a Trust or school laptop containing non-encrypted personal data about pupils.

It is important to note that the Trust and its schools could be reported to the Information Commissioner's Office (ICO) for high-risk data breaches and penalties (including financial) may apply.

18. Training

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

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

19. Monitoring Arrangements

This policy will be reviewed and updated **every year** and shared with the full board of Trustees.

20. Links with Other Policies

This data protection policy is linked to our:

- Staff and Pupil Privacy Notices.
- Data Breach Policy.
- Data Retention Policy.

21. Document Version Control Log

Approver	The Board
Date of approval	
Policy owner	Executive Director of People and Culture
Policy authors	Executive Director of People and Culture
Version	2.0
Date of next review	January 2029
Summary of changes in this review	• Aligned and written to the example and guidance provided by our new DPO School Pro.
Related policies and documents	• Retention policy • Breach policy • Privacy notices