Learning for Life
Stronger together

DATA PROTECTION POLICY

This policy is written in accordance with the requirements of the General Data Protection Regulation ("GDPR"). This policy applies to all personal data, regardless of whether it is in paper or electronic format. The policy reflects the ICO's code of practice for the use of surveillance cameras and personal information.

Contents

1. Policy Statement 2
2. Definition of data protection terms 2
2.2 The data controller 3
3. Roles and responsibilities 3
3.2 Board of Directors 3
3.3 Data Protection Officer 3
3.4 Headteacher 3
3.5 All staff 3
4. Data Protection Principles 4
4.2 Fair and lawful processing of personal data 4
4.3 Privacy notices 5
4.4 Consent to personal data processing 5
4.5 Consent forms 5
4.6 Limitation, minimisation and accuracy 6
5. Sharing personal data 6
6. The rights of an individual over their data 6
6.2 Subject Access Requests 6
6.3 Responding to subject access requests 7
6.4 Other data protection rights of the individual 8
7. Parental requests to see the educational record of their child 8
8. Data security and storage of records 9
9. Disposal of records 9
10. Data Protection by design and default 9
11. CCTV 10
12. Photographs and videos 10
13. Personal data breaches 10
14. Links with other policies / documents 10
15. Policy Review 11

1. Policy Statement

This document is a statement of the aims and principles of the Learning for Life Education Trust (hereinafter called the Trust) for ensuring the correct handling and protection of personal information relating to staff, pupils, parents, directors and local governance committees (LGCs).

As a Trust, we are committed to protecting all the personal data and special category personal data for which we are a data controller.

This policy and any other documents referred to in it set out the basis on which we will process all personal data we collect from data subjects, or that is provided to us by data subjects or other sources – whether this data is handled on computer or manual paper files.

This policy does not form part of any employee's contract of employment and may be amended at any time.

2. Definition of data protection terms

The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('GDPR'), the Data Protection Act 2018, and other regulations (together 'Data Protection Legislation').

The terms below are used in data protection legislation and this policy.

Term	**Definition**
Personal data	Any information relating to an identified, or identifiable, individual. For example name, address, identification numbers.
Special category personal data	Personal data which is more sensitive and 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 which is done to personal data, such as: collecting, storing, organizing, using, altering, disseminating, erasing or destroying. Processing can either be done manually or via automation.
Data subject	The identified or identifiable individual whose data personal data is held
Data Controllers	The people or organizations who determine the purpose and means of processing personal data.
Data users	A member of our workforce (including Governors, Directors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Data processor	A person or body, other than an employee or 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, unauthorized disclosure of, or access to personal data.

2.2 The data controller

Our schools and Trust process personal data relating to parents, pupils, staff, governors, visitors and others, and are therefore data controllers. The schools and Trust are registered as a data controller with the Information Commissioner's Office (ICO) and renew this registration annually or as otherwise legally required.

3. Roles and responsibilities

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

3.2 Board of Directors

The Board of Directors has overall responsibility for ensuring that our schools and the Trust comply with all relevant data protection obligations.

3.3 Data Protection Officer

As a Trust, we are required to appoint a Data Protection Officer ("DPO"). The Data Protection Officer is Louise Peerless, Learning for Life Education Trust and can be contacted at the Trust Office, Irthlingborough Junior School, College Street, Irthlingborough, NN9 5TX. Telephone 01933 654921. Alternatively email dpo@iflt.org.uk.

The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

The DPO is also the central point or contact for all data subjects and others in relation to matters of data protection.

3.4 Headteacher

The headteacher acts as the representative of the data controller on a day to day basis

3.5 All staff

This policy covers all members of staff. For the purposes of this policy, the term staff covers all members of Trust staff (regardless of the employment contract terms), governors, directors, any staff on work placements, volunteers, third party representatives, agency workers.

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with the data protection principles in section 4 of this policy
- Informing the school 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 involve the personal data or privacy rights of any individuals
- If they need help with any contracts or sharing personal data with third parties

4. Data Protection Principles

Anyone processing personal data must comply with the principles are set down in data protection legislation. These state that personal data must:

- Be obtained and processed fairly and transparently in relation to the data subject;
- Be obtained and processed for a specified, lawful purposes and shall not be processed in any manner incompatible with these purposes;
- Be adequate, relevant and not excessive for that purpose;
- Be accurate and kept up to date;
- Not be kept for longer than is necessary;
- Processed securely using appropriate technical and organizational measures;
- Be processed in line with the data subjects' rights
- Not be transferred to people or organisations situated in other countries without adequate protection.

4.2 Fair and lawful processing of personal data

Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

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

- that the personal data is being processed;
- why the personal data is being processed;
- what the lawful basis is for that processing (see below);
- whether the personal data will be shared, and if so with whom;
- the period for which the data will be held;
- the existence of the data subject's rights in relation to the processing of that personal data
- the right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. We will only process personal data under the following legal grounds:

- where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract;
- where the processing is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011);
- the data needs to be processed to ensure that the vital interests of the individual eg to protect someone's life
- where the law otherwise allows us to process the personal data or we are carrying out a task in the public interest;
- the data needs to be processed for the legitimate interests of the school or a 3rd 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 (see below).

When special category personal data is being processed, then an additional legal ground must apply to that processing. We will normally only process special category personal data under following legal grounds:

- where the processing is necessary for employment law purposes, for example in relation to sickness absence;
- where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- where the processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and
- where none of the above applies then we will seek the consent of the data subject to the processing of their special category personal data.

4.3 Privacy notices

We use privacy notices, as required by data protection law, to inform data subjects of the above matters. We will issue privacy notices within one month of the first point of data collection for a subject.

4.4 Consent to personal data processing

Where none of the legal bases for processing set out above apply, then the school must seek the consent of the data subject before processing any personal data for any purpose.
There are strict legal requirements in relation to the form of consent that must be obtained from data subjects. Where we require consent for any processing of personal data, we must:

- Inform the data subject of exactly what we intend to do with their personal data;
- Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
- Inform the data subject of how they can withdraw their consent.

Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

A record must always be kept of any consent, including how it was obtained and when.

4.5 Consent forms

When we need to gather consents from a data subject, we will use a consent form.

The consents given via these forms stand for the duration of the data subject's involvement with the Trust. Should the data subject wish to withdraw consent at any time, they can do so by contacting the school office.

The DPO must always be consulted in relation to any consent form before consent is obtained.

When pupils/employees join the Trust a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things.

4.6 Limitation, minimisation and accuracy

We will only obtain personal data that is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any processing.

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

We will take reasonable steps to ensure that the personal data we hold is accurate and kept up to date, and to destroy or amend inaccurate or out of date personal data.

When staff no longer need the personal data that they hold, they must ensure that it is deleted or anonymised. This will be done in accordance with Trust Record Management Policy.

In terms of emergency contact details we hold, it is the responsibility of the parent/carer to inform any third party or other contact they give that they have passed their data on to the Trust/school.

5. 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 will seek consent as necessary before doing this, unless
- there is a concern for the welfare of the child.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for
- example, our Payroll provider. When doing this, we will:
    - Only appoint suppliers or contractors who 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 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.

6. The rights of an individual over their data

6.2 Subject Access Requests

Individuals have the right to make a subject access request to the personal data that we hold about them. This includes:

- Confirmation that their personal data is being held and/or processed

- Access to a copy of the data
- The purpose for this data to be held/processed
- 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 not possible, the criteria used to determine this period
- The source of the data – if it was not from the individual themselves
- Whether any automated decision making is being applied to their data, and what the significance and consequence of this might be for the individual

Subject Access Requests must in the first instance be submitted in writing, either by letter or email, to the school office concerned. The request must then be given to the Data Protection Officer. The Subject Access Request should include:

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

If any other school staff receive a subject access request, they must forward it to the school office.

Personal data about a child belongs to the child, 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 able 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 subject access request. Therefore, most subject access requests from parents or carers of children 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.

In relation to all pupils under the age of 12 years old, we will seek consent from an individual with parental responsibility for that pupil.

6.3 Responding to subject access requests

The data needed for the subject access request will be gathered by the Headteacher of the school concerned. The Data Protection Officer must be made aware of any requests received and the types of information requested and released. Records must be kept of requests made, and information provided.

When responding to requests, we may:

- Ask the individual to prove their identity by providing forms of identification;
- May contact the individual by phone or letter to confirm the request was made;
- Will respond without delay and within one month of receipt of the request;
- Will provide the information free of charge;
- If the request is complex or numerous, we may tell the individual that we will comply within 3 months of the receipt. Where this happens, we will inform the individual of the extension needed within the first month and explain why the extension is needed.

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 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

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 inform them that they have the right to complain to the ICO.

6.4 Other data protection rights of the individual

In addition to the right to make subject access requests (above) and to receive information when we are collecting their data (Privacy notices), individuals also have the right to:

- Withdraw their consent to processing at any time – this applies where there was no legal basis for the data processing, and consent was given by the individual instead;
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- Prevent the use of their personal data for direct marketing purposes;
- Challenge or object to processing which has been justified on one of the legal bases;
    - In this case, the Trust has to consider the compelling legitimate grounds for processing the information, which may override the rights of the data subject, in deciding whether to uphold the objection;
    - Some such circumstances may be complex and must be referred to the Data Protection Officer
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions made solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively impact 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 DPO. If any other staff receive such a request, they must immediately forward it to the DPO.

7. Parental requests to see the educational record of their child

Parents may request to see the educational records of their child. These are the official records for which headteachers are responsible. They include copies of reports about the child's achievements, and other records about these achievements, exchanges of letters and any information which the school has received from the local authority regarding the child's education. The education records do not include the notes that a teacher may make for his or her own use only. There may be other records kept by the school, such as details of behaviour and family background, but these notes are not compulsory and as such do not form part of 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 school days of receipt of a written request. The request should be addressed to the headteacher of the school.

Whilst in principle, parents/guardians have the right of access to the whole of their child's educational records, in exceptional circumstances some information may be withheld, such as:

- Information which might cause harm to the parent/guardian's physical or mental health or that of a third party;

- Information which may identify third parties, for example other pupils, although not teachers;
- Information which forms part of some court reports
- Information that, if revealed, would hinder the prevention and detection of crime.

There is no charge for a parent/guardian to view their child's records. However, the schools may charge if asked to provide a paper copy of the records. Charges depend on the number of pages provided. For example, 1 to 19 pages will cost £1.20; 29 pages will cost £2, and so on, up to a maximum of 500+ pages which will cost £50.

8. Data security and storage of records

We will take appropriate security measures in processing and protecting personal data.
Security procedures in place include:

- Data Protection specific elements in our code of conduct which each member of staff must adhere to. The codes of conduct do not form part of the contract of employment and as such can be reviewed and changed when necessary. When they are changed, staff will be issued with the new version.
- Staff and children must adhere to the Acceptable Use policies in place at each school
- Staff must adhere to the contents of the staff handbook for each school
- Secure lockable desks and cupboards. Desks and cupboards that hold confidential information of any kind should be kept locked. It is the individual responsibility of every employee to clear their desk of any confidential information (which includes any information relating to an identifiable individual)
- Paper documents containing personal or confidential information must be shredded.
- Digital storage devices and IT assets must be disposed of in accordance with the Information Commissioner's Office guidelines when they are no longer required. We may use a 3rd party to carry out this work. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.
- Any member of staff found to be in breach of the security measures may be subject to disciplinary action.

9. Disposal of records

Personal data that is no longer needed will be disposed of securely according to our Records Management policy. Personal data that has become inaccurate or out of data 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 use a third party to dispose of records or IT equipment on our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

10. Data Protection by design and default

The Trust will consider and comply with the principles of 'data protection by design' in its personal data processing activities.

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 4);
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies.

    - The Trust will complete an assessment of any such proposed processing, recording on a template document to ensure that all relevant matters are considered.
    - The DPO should always be consulted as to whether to a data protection impact assessment is needed, and for guidance on how to undertake the assessment.
- 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
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school 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

11. CCTV

We use CCTV in various locations around our school sites to ensure that they remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask an individual's 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 should be directed to the Headteacher of the school.

12. Photographs and videos

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

We will obtain written consent from parents/carers for photographs and videos of their child to be used for communication, marketing and promotional materials. This will be done via the consent form when the pupil starts at the school. Consent can be withdrawn at any time. If consent is withdrawn, we will delete any photographs or videos from such materials and not distribute further.

13. Personal data breaches

The Trust takes data protection very seriously and 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 Trust Personal Data Breach Reporting Procedure. When appropriate, we will report the data breach to the ICO within 72 hours.

14. Links with other policies / documents

Trust Personal Data Breach Reporting Procedure
Trust and school Safeguarding policy
Safer recruitment and selection policy
Trust Records Management Policy

15.Policy Review

This policy will be reviewed annually. Where any clarifications or actions are needed, the policy will be amended accordingly in line with government policy.

Signed: ……. Dated: ……
Chair, Board of Directors Risk and Audit Committee