GDPR Policy

Contents

1. Aims
2. Legislation and guidance
3. Definitions
4. Roles and responsibilities
5. Data protection principles
6. Collecting personal data
7. Sharing personal data
8. Photographs and videos
9. Data protection by design and default
10. Data security and storage of records
11. Strategic and operational principles
12. Technical solutions
13. Disposal of records
14. Personal data breaches
15. Monitoring and training

East Hall Farmhouse
St Pauls Walden
Hitchin
SG4 8DJ

Reviewed: September 2020
Next Review: July 2021

Aims

Learning to Listen aims to ensure that all personal data collected about staff, pupils, parents, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives those with parental responsibility the right of access to their child/young person's educational record.

Definitions

Any information relating to an identified, or identifiable, individual. This may include the individual's:

Personal data

- 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.

Roles and responsibilities

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

Company Director
The director has overall responsibility for ensuring that our centre complies with all relevant data protection obligations and acts as the Data Controller on a day-to-day-basis.

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. The DPO is also the first point of contact for individuals whose data the centre processes, Our DPO is Jo Osborn and is contactable by email jo.osborn@learningtolisten.co.uk

All staff

Staff are responsible for:

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

Staff are also responsible for contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the 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

Data protection principles

The GDPR is based on data protection principles that our centre 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 to be 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

Collecting personal data

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 centre can fulfil a contract with the individual, or the individual has asked the centre to take specific steps before entering into a contract

• The data needs to be processed so that the centre 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 so that the centre , as a public authority, can perform a task in the public interest, and carry out its official functions

• The data needs to be processed for the legitimate interests of the centre or a third party (provided the individual's rights and freedoms are not overridden)

• The individual (or the person with parental responsibility when appropriate in the case of a child/ young person) has freely given clear consent

• For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

• If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the child is under 13. If the child/young person is aged 13 and above we may get their consent, as considered appropriate.

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

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 guidance from the Information and Records Management Society's toolkit for centre s.

Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

• There is an issue with a child/young person or person with parental responsibility 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 children/ young people –for example, IT companies. 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 stand-alone 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.

Subject access requests and other rights of individuals

Subject access requests (SAR)

Individuals have a right to make a 'subject access request' to gain access to personal information that the centre 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

• 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 must 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 the DPO

Children and subject access requests

Personal data about a child belongs to that child, and not the person with parental responsibility for the child. For a person with parental responsibility for the child to make a subject access request with respect to the child they have responsibility for, 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 a person with parental responsibility for the child may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

Children/young people aged 12 and above can generally be regarded as able enough to understand their rights and the implications of a subject access request, dependent on the child/young person. Therefore, subject access requests from persons with parental responsibility for the child/young person at our centre may not be granted without the express permission of the child/young person. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by case basis.

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 child/young person or another individual
- Would reveal that the child/young person is at risk of abuse, where the disclosure of that information would not be in the child/young person's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child/young person

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, 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

Photographs and videos

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

We will obtain written consent from those with parental responsibility, or young people aged 18 and over, as appropriate, for photographs and videos to be taken of young people for communication, marketing and promotional materials, etc.

Where we need consent from those with parental responsibility, we will clearly explain how the photograph and/or video will be used to both those with parental responsibility and the young person, as appropriate. Where we don't need parental consent, we will clearly explain to the young person how the photograph and/or video will be used.

Uses may include:

• Videoed by the centre for use to assist with reflective practice for staff

• Photographed by the centre (e.g. communication boards and internal displays).

• Photographed by the centre for use on the website.

• Photographs used in local press i.e. centre events.

• Videoed by the centre during centre productions that may be used on the centre website and for external presentations.

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 accompany them with any other personal information about the child, to ensure they cannot be identified.

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 section6)

• Completing privacy impact assessments where the centre '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

Maintaining records of our processing activities, including:

• For the benefit of data subjects, making available the name and contact details of our centre 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

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.

Strategic and operational practices

• Jo Osborn is the Data Protection Officer (DPO) with responsibility for data protection compliance.

• Staff are clear who the key contacts for key centre information are.

• We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.

• All staff are DBS checked and records are held in one central record.

• We monitor centre e-mails, etc to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails, etc.

• We follow LA guidelines for the transfer of any data, such as reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.

• All staff have their own unique username and private passwords to access centre systems. Staff are responsible for keeping their passwords private.

• We require staff to use strong passwords

• We require that any personal/sensitive material must be encrypted if the material is to be removed from the centre and limit such data removal.

Technical or manual solutions

• Staff must use secure data storage for sensitive documents.

• We store any sensitive/special category written material in lockable storage cabinets in a locked office.

• All backup drives are stored in secure, locked locations.

• We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.

• Paper based sensitive information is shredded, using a cross-cut shredder or incineration.

• Paper-based records and portable electronic devices, such as laptops and hard drives are stored in locked metal cabinets in locked office when not in use.

• We enforce a clear desk policy (sensitive documents must be locked away when the user's desk is unattended).

• Where possible, all storage devices that contain sensitive data must be encrypted.

• Staff and students are not permitted to store information on their personal portable devices (see our Device 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.

• Emails sent out of the organisation containing sensitive data must be encrypted using Egress Switch encryption software; internal emails are sent through our dedicated secure email server.

• Anti-virus software is used on all computers and is freely available for staff to install on their home computers.

• Staff must not transfer/store any centre data (pupil/staff info/photos/videos, etc) to any Cloud service, e.g. DropBox, ICloud, Google Drive, Microsoft OneDrive, etc.

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

Personal data breaches

The centre will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, when appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a centre context may include, but are not limited to:

• Safeguarding information being made available to an unauthorised person

• The theft of a centre laptop containing non-encrypted personal data about children/young people

Training and Monitoring Training

All staff 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 centre 's processes make it necessary

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our centre 's practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full governing board.

Note: the 2-year review frequency here reflects the information in the Department for Education's advice on statutory policies. While the GDPR and Data Protection Act 2018 (when in place) are still new and centres are working out how best to implement them, you may wish to review your data protection policy annually, and then extend this to every 2 years once you are confident with your arrangements.