

Data Protection Policy

Context and overview

Key details

- Policy prepared by: Sarah Mackay
- Approved by: Glynis Frater / Director
- Policy became operational on: 25th May 2018
- Next review date: 24th May 2019

Introduction

Learning Cultures Limited stores information about full-time and part-time staff, consultants and trainers

Learning Cultures Limited needs to gather, use and store certain information about organisations especially schools, colleges and related companies and the individuals with specific roles within those organisations. We do not hold the personal data for individuals except in their capacity within a school, college or other related company.

The information we hold will include customers, suppliers, business contacts employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet Learning Cultures' data protection standards and to comply with the law.

Why this policy exists

The Data Protection Act 1998 describes how organisations including Learning Cultures Limited must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law. Personal information must be collected and used fairly. Stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA) unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

- The registered office of Learning Cultures Limited
- The Coaching School and offices of Learning Cultures Limited
- All staff, trainers, consultants and volunteers of Learning Cultures Limited
- All contractors, suppliers and other people working on behalf of Learning Cultures Limited
- The information we hold relating to our customers and suppliers and their representatives

The policy applies to all data Learning Cultures Limited holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Name of individuals
- Postal addresses
- Email addresses
- Telephone numbers

Data protection risks

This policy helps to protect Learning Cultures Limited from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Learning Cultures Limited has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Board of Directors** is ultimately responsible for ensuring that Learning Cultures Limited meets its legal obligation
- The **Data Protection Officer** Sarah Mackay is responsible for:
 - Keeping the board updated about data protection responsibilities, risks and issues
 - Reviewing all data protection procedures and related policies, in line with an agreed schedule
 - Arranging data protection training and advice for the people covered by this policy
 - Handling data protection questions from staff and anyone else covered by this policy
 - Dealing with requests from individuals to see that data Learning Cultures Limited holds about them (also called subject access requests)
 - Checking and approving any contracts or agreements with third parties that may handle the sensitive data held by Learning Cultures Limited
- The **IT Contractor** Crawford Coulson is responsible for
 - Ensuring all systems, services and equipment used for storing data meet acceptable security standards
 - Performing regular checks and scans to ensure security hardware and software is functioning properly
 - Evaluating any third-parties the company uses such as cloud computing services
- The **Marketing Manager** Glynis Frater is responsible for:
 - Approving any data protection statements attached to communications such as emails and letters
 - Addressing any data protection queries from journalists or media outlets like newspapers
 - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for work**
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers
- Learning Cultures Limited **will provide training** to all employees to help them understand their responsibilities when handling data
- Employees will **keep all data secure**, by taking sensible precautions and following the guidelines below
- In particular, **strong passwords must be used** and they will never be shared
- Personal data **will not be disclosed** to unauthorised people, either within the company or externally
- Data is **regularly reviewed and updated** if it is found to be out of date. If no longer required, it will be deleted and disposed of
- Employees **should request help** from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection

Data storage

These rules describe how and where data is safely stored. Questions about storing data safely can be directed to the IT Manager or Data Protection Officer

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed for some reason:

- When not required, the paper or files will be kept **in a locked drawer or filing cabinet**.
- Employees will make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer
- **Data printouts should be shredded** and disposed of securely when no longer required

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data is **protected by strong passwords** that are changed regularly (every three months) and never shared between employees
- If data is **stored on removable media** (like CD or DVD), it is kept locked away securely when not being used
- Data is stored on **designated drives and servers, (Y-Drive)** and is only uploaded to our approved cloud office space
- Servers containing personal data are **sited in a secure location**, away from general office space
- Data is **backed up daily and weekly**. The backups are tested regularly, in line with Learning Cultures' standard back up procedures for all our IT operations
- Data is **not saved directly** to laptops or other mobile devices like tablets or smart phones
- All servers and computers containing data are protected by **approved security software and a firewall**

Data use

Personal data is not used as part of our business operations. The personal data of our staff, trainers and consultants is important to us. However, we take great care to ensure that it is carefully secured to avoid risk of loss, corruption or theft and our staff follow the following guidelines:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure
- Data must be **encrypted before being transferred electronically**. The IT Manager is responsible for sending data to authorised external contacts
- Personal data should **never be transferred outside the European Economic Area**
- Employees **should not save copies of personal data to their own computers**. Data access is always made through the updating of the central data base
- The data we use with customers, those making enquiries and visitors to our website is not personal to an individual, except to say that we keep their name and job title and their email address relating to their place of work. We carry no personal emails or telephone numbers or other personal information unless they are given with the individual's express permission. If this is the case the same detailed care is taken as with information about our own staff, consultants and trainers
- The data we keep relating to schools, colleges and other companies to whom we provide consultancy, training and development services is in the public domain. It is stored with the same care as all our other data and is updated and reviewed with the same rigour

Data Accuracy

We acknowledge that the law requires Learning Cultures Limited to take reasonable steps to ensure data is kept accurate and up to-date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets
- Staff are instructed to **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call or updating an email address when it changes
- Learning Cultures Limited will make it **easy for data subjects to update their information** Learning Cultures holds for them. Generally, this is through access to a variety of contact forms available on our website
- Data is **updated as inaccuracies are discovered**. For instance, if a customer's email address is recorded inaccurately this is updated immediately
- It is the Marketing Manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months
- Where an individual from a school, college or company unsubscribes **their record is tagged as unsubscribe**
- Where a school, college or company unsubscribes their generic email address we **endeavour to discuss this and to find an individual to whom our services may be relevant**

Subject access requests

All individuals who are the subject of personal data held by Learning Cultures Limited are entitled to:

- Ask **what information** the company holds about them and why
- Ask **how to gain access** to it
- Be informed how the company is **meeting its data protection obligations**

If individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at 12a Northgate, Bridgnorth WV16 4ER. The Data Protection Officer can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10.00 per subject access request. The Data Protection Officer will aim to provide the relevant data within 14 days.

The Data Protection Officer will always verify the identity of anyone making a subject access request before handing over any information

Disclosing data for other reasons

In certain circumstances the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject

Under these circumstances Learning Cultures Limited will disclose the requested data. However, the Data Protection Officer will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Learning Cultures Limited aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy policy, setting out how the data relating to individuals is being used by the company

A version of this Data Protection Policy and our Privacy Policy are both available on our website

www.learningcultures.org