

DATA PROTECTION POLICY



Policy Group: Data Protection, Security, and Information

Effective: November 2024

Approved: Taya Reynolds, Chief Technology Officer

Responsible Officer: Neil Whittaker, Director of Marketing and Communications

Next Renew Date: November 2025

Ref no: 5.1



GUIDANCE

Vision

Transform lives through learning

Values



PASSIONATE - We are passionate about inspiring young people, adults and our Purple People to be their best and we take pride in creating a positive learning environment to fulfil their potential.



UNSTOPPABLE - We are unstoppable in our quest for the pursuit of excellence. We are dedicated and resilient to develop ourselves and our learners.



RIGHT - We treat each other with respect and strive to do the right thing through insight, inclusion, honesty, growth and trustworthiness.



PARTNERSHIPS - We support the people surrounding us in our everyday lives, building effective partnerships with businesses, learners and all stakeholders where we can pass on our knowledge and skills to help them meet their goals.



LEARNERS - Learners are at the centre of everything we do and we are driven to provide life-changing and life-long learning for them.



EMPOWERED - We encourage our Purple People to be independent and autonomous to maximise their goals surpassing their barriers and targets. Feel it, believe it, live it.

Tone of voice

Our tone of voice takes its direct influence from our core values. We are passionate about people and learners and are driven to get the best out of everyone by understanding them. We are caring and supportive, as well as being determined and striving for growth. We talk with purpose and enthusiasm in a way that connects and empowers people.

Innovation is at the heart of Learning Curve Group and we're always thinking about what's next!

SUMMARY CHANGES

Date	Page	Details of Amendments
May 2020	5	Update the 7 Principles of Data Protection
Nov 2022		Contact information updated
Novr 2022	23	Appendix 2 – Data Subject Access Request Form added
Mar 2023	4	Update to Introduction
Dec 2023	All	Annual Review
Nov 2024	All	Annual Review

INTRODUCTION

Learning Curve Group (LCG) is one of the largest national training providers in the UK, providing education and training nationally. All companies within the LCG family uphold the same company Vision, Mission and Core Values and follow our group policies and procedures.

Applies to

This policy applies to all the processing of personal data carried out by Learning Curve Group being a controller of data and including processing carried out as a joint controller and as an agreed processor. We collect and use personal information, and this policy applies to the personal data of:

- Learners, service users, customers
- Relatives of any of the forgoing
- Suppliers

Reason for policy

To ensure Learning Curve Group comply with its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18).

Please note that the following inter-changeable terms, are used throughout this document:

- Personal data and personally identifiable information (PII)
- Data subject and individual
- Regulator and Information Commissioners Office – ICO

POLICY

This policy sets out how we comply with our data protection obligations and seek to protect personally identifiable information. Its purpose is to ensure that employees understand and comply with the rules governing the collection, use and deletion of personal information to which they have access to in the course of their work.

The policy does not form part of the formal contract of employment, but it is a condition of engagement that employers, employees, contractors, and associates abide by the rules and policies made. Any failures to follow this policy can therefore result in disciplinary action.

The Director of Marketing & Communications is responsible for data protection compliance within Learning Curve Group. If you have any questions or comments about the content of this policy or if you need further information, you should contact the Director of Marketing & Communications on data.protection@learningcurvegroup.co.uk or 01388 777 129.

We regard the lawful and correct treatment of personal information as very important to our successful operations and to maintaining confidence between Learning Curve Group and those with whom it carries out business with. We will ensure that we treat personal information lawfully and correctly.

Personal information will be handled and dealt with properly however it is collected, recorded, and used, and whether it be on paper, in computer records or recorded by any other means.

As part of our commitment to data protection, we will review and update this policy regularly in accordance with our data protection obligations. We may amend, update, or supplement it from time to time. We will circulate any new or modified policy to employees when it is adopted.

The 7 Principles of Data Protection

We will comply with the following seven data protection principles when processing personal identifiable information:

1. We will process information fairly, lawfully and in a transparent manner.
2. We will collect personal information for specified, explicit and legitimate purposes only, and will not process it in any manner incompatible with those legitimate purposes.
3. We will only process the personal information that is adequate, relevant, and necessary for the relevant purposes.
4. We will keep accurate and up to date personal information and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay.
5. We will keep personal information for no longer than is necessary for the purposes for which the information is processed.
6. We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.
7. We will ensure that all employees are trained and are held accountable when processing personal information, to ensure that we do not put individuals at risk because of processing their personal data.

Basis for Processing Personal Information

In relation to any processing activity, we will, before the processing starts for the first time and then regularly while it continues, review the purposes of the processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

1. That the data subject has consented to the processing.
2. That the processing is necessary for the performance of a contract to which the data is required.
3. Subject is party or to take steps at the request of the data subject prior to entering a contract.
4. That the processing is necessary for compliance with a legal obligation to which Learning Curve Group is subject.
5. That the processing is necessary for the protection of the vital interests of the data subject or another natural person.
6. That the processing is necessary for the purposes of legitimate interests of Learning Curve Group or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

Except where the processing is based on consent, we will:

1. Satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).
2. Document our decision as to which lawful basis applies, to help demonstrate our compliance with the 7 Data Protection Principles.
3. Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s).
4. Where special category personal information is processed, also identify a lawful special condition for processing that information and document it.
5. Where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

When determining whether Learning Curve Groups legitimate interests are the most appropriate basis for lawful processing, we will:

1. Conduct a legitimate interest assessment (LIA) and keep a record of it, to ensure that we can justify our decision.
2. If the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA)
3. Keep the LIA under review and repeat it if circumstances change.
4. Include information about our legitimate interests in our relevant notice(s)

Special Category Personal Information

A special category of personal data is afforded stronger protection under the UK GDPR and the DPA 2018 than ordinary personal data. This personal data by its nature is more sensitive and is afforded more protection, this is information related to:

1. Race or ethnic origin.
2. Political opinions.
3. Religious or philosophical beliefs.
4. Trade union membership.
5. Genetic data.

6. Biometric ID data.
7. Health data.
8. Sexual life and/or sexual orientation.
9. Criminal offence data (convictions and offences).

Before processing any special category personal information, employees must notify the Director of Marketing & Communications of the proposed processing, in order that the Director of Marketing & Communications may assess whether the processing complies with the criteria noted above.

Special category personal information will not be processed until:

1. The assessment above has taken place; and
2. The individual has been properly informed (by the way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Privacy Notice

Learning Curve Group will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible, and easily accessible form, using clear and plain language and our full notices is currently on our website alongside a guide on how we use cookies.

We take your privacy very seriously and would request you read this privacy policy carefully as it contains important information on who we are and how and why we collect, store, use and share your personal data. It also explains your rights in relation to your personal data and how to contact us or the Information Commissioners Office in the event you have a complaint.

Individual Rights

You have the following rights in relation to your personal information:

- To be informed about how, why and on what basis that information is processed.
- To obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request using the [Data Protection Submission Form](#)
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten'). By making a deletion of personal data request using the [Data Protection Submission Form](#)
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased).

If you wish to exercise any of the rights above, please fill in the Data Protection Submission Form and fill in the relevant section such as unsubscribe, data deletion, subject access request or data breach. You can also make the requests by email to data.protection@learningcurvegroup or by calling Learning Curve Group.

Information Security

Learning Curve Group will use appropriate technical and organisational measures to keep personal information secure, and to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

International Transfers

Learning Curve Group will not transfer personal information outside of the United Kingdom.

Storage and Retention of Personal Information

Personal information (and special category personal information) will not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Employees follow Learning Curve Groups 5.9 Data Retention and Archiving Policy and Process which sets out the relevant retention periods. Where there is any uncertainty, employees should consult the Director of Marketing & Communications.

Disposing of Data

Data will be disposed of through either confidential shredding using an external contractor or purging from the company devices/servers.

Where computer equipment is disposed of, all data shall be removed and storage media such as hard disks, tablets, iPads, mobile phones, and USB memory sticks will be “electronically” shredded or a similar procedure to ensure that data can’t be “reclaimed”. Learning Curve Group will only use a fully certified WEEE compliant company who provide us with secure data destruction services.

Data Breaches

Learning Curve Group takes every care in protecting the personal information it holds and avoiding risks which could lead to a compromise of security and a potential data protection breach. Compromised security and/or data breaches can result in harm to the individual(s) involved, reputational damage to the Learning Curve Group, detrimental effect on service provision, legislative non-compliance, and/or financial costs. For further guidance on the proper procedure of reporting a data breach refer to 5.1.1 Data Breach Procedure.

Training

Learning Curve Group will ensure that employees are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests, will receive additional training to help them understand their duties under Article 15 UK GDPR and how to comply with them.

All Learning Curve employees undertake a Data Protection and Information Security E-Learning module on induction. Then all employees are required to complete yearly continuing professional development (CPD) that also covers a refresher on data protection.

Consequences of Failing to Comply

The Company takes compliance with this policy very seriously. Failure to comply with the policy:

- Puts at risk the individuals whose personal information is being processed; and
- Carries the risk of significant civil and criminal sanctions for the individual and the Company; and
- May, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Director of Marketing & Communications.

Definitions

Criminal offence data – means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

Data breach – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal information.

Data subject – means the individual to whom the personal information relates.

Personal data - means information relating to an individual who can be identified (directly or indirectly) from that information. Data that, if lost or stolen, would be likely to cause damage or distress to one or more individuals. This includes, but is not limited to name, address, bank details, NI number, medical history which are not a matter of public record.

Controller – meaning the body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processing information – means obtaining, recording, organising, storing, amending, retrieving, disclosing and / or destroying information, or using or doing anything with it.

Special category information – means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

POLICY REVIEW

This policy will be updated by Learning Curve Group as necessary to reflect best practice and to ensure compliance with any changes or amendments to the Data Protection Act 2018.

RELATED POLICIES

- 5.1.1 Data Breach Procedure
- 5.2 IT Acceptable Use Policy
- 5.2.4 Bring Your Own Device Policy (BYOD)
- 5.6 Information Security Policy
- 5.8 Data Classification Policy
- 5.9 Data Retention and Archiving Policy and Process
- 5.9.1 Record Retention Schedule