DATA BREACH PROCEDURE

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: 5.1.1

GUIDANCE

Vision

Transform lives through learning

Values

P — 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.

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

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

P — 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.

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

E — 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		Reflect LHAA
May 2021	Whole document	Annual Review
Nov 2022		Contact details updated
Nov 2022	8	Appendix 1 - Data Breach Report Form added
Mar 2023	4	Update to Introduction
Nov 2023	All	Adding Data Protection Team, Changing the Company to Learning Curve Group, Updating the Data Protection Submission form and removing Appendix A.
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.

Learning Curve Group collects, holds, processes, and shares information and we are aware personal information is an asset. We must protect all personally Identifiable information we hold from either accidental or deliberate incidents, which could lead to a data protection breach.

Applies to

This policy shall apply to all employees, contractors, learners, and associates of Learning Curve Group, including temporary, casual or agency staff and, consultants, suppliers, and data processors working for, or on behalf of Learning Curve Group.

Reason for procedure

We are obliged under Data Protection legislation to have in place a framework designed to ensure the security of all personal information, including clear lines of responsibility.

This procedure must be followed to ensure a consistent and effective approach is in place for managing data breaches across LCG. It relates to all personal and sensitive personal information held by us regardless of format. The objective of this procedure is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal information and prevent further breaches.

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

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

This policy and procedure do not form part of your terms and conditions of employment and can be changed at any time as we deem appropriate.

PROCEDURE

Reporting

We recognise damage limitation is a priority immediately following a security incident/breach.

Any individual who accesses, uses, or manages Learning Curve Groups information/data is responsible for reporting a data breach and security incidents immediately to the Data Protection Team at data.protection@learningcurvegroup.co.uk

If a breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable to the Data Protection Team for member see Appendix 1, and the Director of Marketing and Communications who heads up this team.

The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting, the nature of the information, and how many individuals are involved. A Data Breach Report should be completed by filling in this Data Protection Submission Form.

The report will enable the Data Protection Team to make the decision as to whether to inform any affected individuals and the Information Commissioners Office (ICO), about the breach. The time limit for notifying the ICO is 72 hours from becoming aware of the breach and it is best practice to inform the regulator first before communicating with those affected. Therefore, any individual reporting a breach or security incident must act with urgency and provide as much information as possible in the Data Protection Submission Form.

Preliminary Assessment, Containment and Recovery

The Data Protection Team will take steps, within the first 24 hours of the incident (where possible) to carry out a preliminary assessment of what data has been lost, why and how. Containment and recovery will then become the priority.

The Data Protection Team will attempt to contain the breach or determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise further loss, destruction, or unauthorised disclosure of data. This will be done in line with the Data Assessment and Action Plan. The Data Protection Team may need to notify Learning Curve Groups insurers and, if the breach arises out of a criminal event notify the police and the National Cyber Security Centre.

Investigation and Risk Assessment

Having dealt with the immediate aftermath of the data breach, the Data Protection Team will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for the data subjects, how serious or substantial those are and how likely they are to occur.

The investigation will need to consider the following:

- The type of data involved.
- Its sensitivity.
- The risk of harm of the data subject.
- What security measures or procedures are in place (e.g., passwords/encryptions).

- What has happened to the data (e.g., has it been lost or stolen).
- Whether the data could be put to any illegal or inappropriate use.
- The individuals affected by the breach, number of individuals involved and the potential effects on those individual(s).
- Whether there are any wider consequences to the breach.

The Data Protection Team will record the breach in the Breach Register (regardless of whether an ICO notification is required or not).

Notification

Every incident will be assessed on a case-by-case basis. The dangers of over notifying must be considered. Not every incident warrants a notification and over notification may cause disproportionate queries and work.

The Data Protection Team will establish whether the ICO will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible. Where there is no risk to the rights and freedoms of the data subjects, the regulator will not be notified.

The Data Protection Team will also establish whether any affected data subjects need to be notified. As above, this notification is only required where the breach is likely to result in a high risk to the rights and freedoms of those data subjects. Learning Curve Group is required to notify the ICO without undue delay, but after notification to the regulator, its best practice to notify those affected and include a description of how and when the breach occurred, and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks by Learning Curve Group.

The Data Protection Team will consider whether anyone else will require notification, e.g., a business party pursuant to a contractual obligation. They also must consider notifying third parties such as the police, insurers, banks, or credit card companies. This is appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

The Data Protection Team will coordinate with the Marketing team where a press release is required and will cooperate with the rest of Learning Curve Group as to how to handle any incoming press enquiries.

Evaluation and Response

Once the initial incident is contained, the Data Protection Team will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where personal data is held and how it is processed.
- Where the biggest risks lie including potential weak points within existing security measures.
- Whether methods of transmission are secure, sharing minimum amount of data necessary.
- Whether additional employee awareness training is required.

If deemed necessary, the Data Protection Team will put forward a report recommending any changes to systems, policies, and procedures, to be considered by Learning Curve Groups Board.

LEGAL & REGULATORY OBLIGATIONS

Learning Curve Group has a responsibility to adhere to all current UK legislation and a variety of regulatory and contractual requirements including:

- Data Protection Act 2018 (UK GDPR)

The requirements of this legislation are reflected in this policy and the supporting policies, procedures, and guidance. By adhering to these instructions, users will ensure that Learning Curve Group complies with its obligations.

CONSEQUENCES OF FAILING TO COMPLY

The company takes compliance with this procedure very seriously. Failure to comply with the procedure:

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

Because of the importance of this procedure, 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 procedure, they may have their contract terminated with immediate effect.

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

DEFINITIONS

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, bank details, human resources data and exam or assessment results which are not a matter of public record.

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, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data subject – means the individual to whom the personally data relates to.

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

Special category information – (sometimes known as 'special categories of personal data' or 'sensitive personal data') 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.

Information Commissioners Office - Is the UK's independent regulator for data protection and upholding information rights and data privacy for individuals. The ICO can act against organisations and individuals that collect, use and keep personal information. This includes criminal prosecution, non-criminal enforcement and audit.

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 Data Breach Policy
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

APPENDIX 1

The Data Protection Team are responsible for ensuring that this procedure is followed in accordance with the Data Protection Act 20 the 5.1 Data Protection Policy.

Table of members

Job Role / Title	Responsibilities
DPO	Ensures LCG compliance with Data Protection law and reporting to the ICO.
IT Security Officer	Investigation and compliance with Data Protection law and reporting to the ICO.
Head of Bids & Contracts	Investigation and compliance with Data Protection law.
Legal Manager	Monitoring of Data Protection mailbox and allocation of requests.
PA to CEO	Monitoring of Data Protection mailbox and investigating requests.
Business analyst	Monitoring of Data Protection mailbox and investigating requests.