

DATA BREACH PROCEDURE



Policy Group: Data Protection, Security, and Information

Effective: November 2022

Approved: Hannah Marshall, Chief Technology Officer

Responsible Officer: Neil Whittaker, Director of Marketing and Communications

Next Renew Date: November 2023

Ref no: 5.1.1



GUIDANCE

Vision

Transform lives through learning

Values



PASSIONATE - We're passionate about everything we do, especially creating as many opportunities as we can for both young people and adults to gain new skills.



UNSTOPPABLE - We are committed to continually exploring ways to improve the service that we offer for the benefit of our learners, partners, and employers.



RIGHT - We endeavour to be open, honest and fair in our dealings with learners, employers, partners and stakeholders. We also aim to get it right first time.



PARTNERSHIPS - We continually strive to deliver excellence through strategic and sustainable partnerships with a wide range of FE organisations, employers and wider stakeholders.



LEARNERS - We keep our learners at the centre of everything we do and we are driven by the desire to provide life-changing opportunities for them.



EMPOWERMENT - We are passionate about supporting Purple People at all levels, empowering them to realise their full potential and progress.

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
November 2022		Contact details updated
November 2022	8	Appendix 1 - Data Breach Report Form added
March 2023	4	Update to Introduction

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.

Company	UKPRN	Registration Number
Learning Curve Group Limited	10008935	05233487
Profound Services Limited	10022358	05969610
Northern Care Training Limited	10013515	05256533
Acorn Training Consultants Limited	10000108	03182459
London Hairdressing Apprenticeship Academy Limited	10035171	07710651
Antrec Limited	10043333	07873541
APCYMRU LIMITED (MPCT)	10000311	07873541
The White Rose School of Beauty and Complementary Therapies Limited	10007484	03172520

Learning Curve Group collects, holds, processes, and shares information and we are aware personal information is a valuable asset. We must suitably protect the personal information we hold, at all times from either accidental or deliberate incidents, which could lead to a data protect breach.

Applies to

All staff within the Company, including temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the Company.

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, used throughout this document:

- Personal data and personal information
- Data subject and individual

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 an Incident

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

Any individual who accesses, uses or manages the Company's information is responsible for reporting data breach and security incidents immediately to the Data Breach Team:

data.protection@learningcurvegroup.co.uk

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable to the Data Breach Team, the Director of Marketing and Communications 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 Form should be completed as part of the reporting process (refer to Appendix 1).

The report will enable the Data Breach Team to make the decision as to whether to inform any affected individuals and the regulator about the breach. The time limit for notifying the regulator 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 Breach Report Form.

Preliminary Assessment, Containment and Recovery

The Data Breach 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 Breach 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 Breach Team may need to notify the Company's insurers and, if the breach arises out of a criminal event, notify the police.

Investigation and Risk Assessment

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

The investigation will need to take into account the following:

- The type of data involved;
- Its sensitivity;
- 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); and
- Whether there are any wider consequences to the breach

The Data Breach Team will need to record the breach in the Breach Register (regardless of whether notification is required).

Notification

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

The Data Breach Team will establish whether the regulator 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 Breach Team will also establish whether any affected data subjects need to be notified. As above, notification is only required where the breach is likely to result in a high risk to the rights and freedoms of those data subjects. Notification is required without undue delay, but after notification to the regulator, is best practice. Notification to the affected data subjects will 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 the Company.

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

Evaluation and Response

Once the initial incident is contained, the Data Breach 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 and personal data is held and there and how it is sorted;
- 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;
- And staff awareness

If deemed necessary, the Data Breach Team will put forward a report recommending any changes to systems, policies and procedures, to be considered by Company's Board.

Policy Review

This policy was last reviewed in November 2022.

This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

Data Breach Report Form

If you know or suspect a personal data breach has occurred, please:

- complete this form, and
- email (data.protection@learningcurvegroup.co.uk) or deliver it to the Director of Marketing & Communications ensuring you mark your email or the form as urgent

Name and contact details of person notifying the actual or suspected breach	<i>[Insert name and contact details]</i> <i>If you wish to submit an anonymous report, leave this section blank.</i>
Dept/manager	<i>[Insert department from which the report emanated and the relevant manager]</i>
Date of actual or suspected breach	<i>[Insert date]</i>
Date of discovery of actual or suspected breach	<i>[Insert date]</i>
Date of this report	<i>[Insert date]</i>
Summary of the facts	<i>[Provide as much information as possible—including the amount, sensitivity and type of data involved]</i>
Cause of the actual or suspected breach	<i>[Provide a detailed account of what happened]</i>
Is the actual or suspected breach ongoing?	<i>[Yes OR No]</i>
Who is or could be affected by the actual or suspected breach?	<i>[Include details of categories and approximate number of data subjects concerned]</i> <i>Do not notify affected data subjects. The data breach team will determine who should be notified and how.</i>
Are you aware of any related or other data breaches?	<i>[Yes OR No]</i> <i>[If yes, provide more details]</i>

This document is issued and controlled by the Director of Performance and Delivery and can only be modified after proposed modifications have been accepted by the Company Directors.

The latest version will be maintained on the company J:Drive under Policies and Procedures.