LEARNING CURVE GROUP

DATA BREACH PROCEDURE

Policy Group: Data Protection, Security and Information

Effective: May 2019

Approved: Gail Crossman, Director of Performance and Development

Responsible officer: Neil Whittaker

Next renew due: May 2020

Ref no.:5.1.1

GUIDANCE

Values | Vision | Tone of Voice

Values

Vision

Transforming lives through learning

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 getting to understand them. We are caring and supportive, as well as being determined and strive 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

I. INTRODUCTION

Learning Curve Group (the 'Company') collects, holds, processes, and shares information. Personal information is a valuable asset. The Company must suitably protect the personal information it holds, at all times from either accidental or deliberate incidents, which could lead to a data protect breach.

Scope

The Company is 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.

The procedure sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breaches across the Company. It relates to all personal and sensitive personal information held by the Company regardless of format.

This procedure is to be applied by 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.
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

II. POLICY

1. Reporting an incident

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 (dataprotection@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 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.

2. 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 pliminary 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.

3. 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).

4. 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.

5. 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, t5o be considered by Company's Board.

6. Policy Review

This policy was last reviewed in May 2018

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

Appendix

Appendix 1: Data Breach Report Form.