LCL Awards Data Breach Policy

1. Introduction

1.1 LCL Awards collects, holds, processes, and shares personal data (that needs to be suitably protected) of employees, learners, teachers, assessors, examiners and internal verifiers associated with LCL Awards awarding managed learning programme and qualification certification to learners.

1.2 Every care is taken by LCL Awards to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise data security.

1.3 Compromise (data breach) of information, confidentiality, integrity, or availability may result in harm to an individual(s), reputational damage, detrimental effect on service provision by LCL Awards, legislative or regulatory non-compliance, and or financial loss.

2. Purpose and Scope

2.1 LCL Awards is required under:

(a) The Data Protection Act 2018;
(b) The Privacy and Electronic Communications (EC Directive) Regulations 2003 (amended 2011)
(c) And any superseding legislation; and all other applicable laws and regulations relating to the processing of personal data and or governing individuals' rights to privacy.

to have in place a formal framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across LCL Awards and its Approved Centres (AC).

2.3 This policy relates to all personal and special categories (sensitive) data held by LCL Awards and its AC regardless of format.

2.4 This policy applies to all LCL Awards and AC staff and their contractors and to learners at AC. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of LCL Awards and or the AC.

2.5 The objective of this policy is to mitigate any data breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

3. Types of breach

3.1 For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

3.2 A breach is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the LCL Awards information assets and or reputation.

3.3 A breach includes but is not restricted to the following:

- 3.3.1 Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad, tablet device, or paper record);
- 3.3.2 Equipment theft or failure;
- 3.3.3 System failure;
- 3.3.4 Unauthorised use of, access to or modification of data or information systems;
- 3.3.5 Attempts (failed or successful) to gain unauthorised access to information or IT system(s);
- 3.3.6 Unauthorised disclosure of sensitive and or confidential data;
- 3.3.7 Website defacement;
- 3.3.8 Hacking attack;
- 3.3.9 Unforeseen circumstances such as a fire or flood;
- 3.3.10 Human error;
- 3.3.11 'Blagging' offences where information is obtained by deceiving either LCL Awards or AC which holds it.

4. Reporting an incident

4.1 Any individual who accesses, uses or manages LCL Awards information is responsible for reporting data breach and information security incidents immediately to compliance@lclawards.co.uk

4.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

4.3 The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. A Data Breach Report Form (DBRF) should be completed as part of the reporting process.

4.4 Staff should be aware that any breach of Data Protection legislation may result in the LCL Awards disciplinary procedures being instigated.

5. Containment and recovery

5.1 The LCL Awards HR Director (HRD) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to mitigate the effect of the breach.

5.2 An initial assessment will be made by the HRD in liaison with relevant managers and or directors to establish the severity of the breach and who will take the lead investigating the breach. An Investigation Officer (IO) (depending on the nature of the breach will be appointed. In some cases the IO may be the HRD).

5.3 The IO will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

5.4 The IO will establish who may need to be notified as part of the initial containment and will with the authority of a member of the Board of Directors (BoD) inform the authorities, where appropriate.

5.5 Advice from experts employed or contracted to LCL Awards may be sought in resolving the incident promptly.

5.6 The IO, in liaison with the relevant manager(s) will determine the suitable course of action to be taken to ensure a resolution to the breach.

6. Investigation and risk assessment

6.1 An investigation will be undertaken by the IO immediately and wherever possible, within 24 hours of the breach being discovered and or reported.

6.2 The IO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

6.3 The investigation will take into account the following:

6.3.1 The type of data involved;
6.3.2 The sensitivity of the data involved;
6.3.3 The protections are in place (e.g. encryptions);
6.3.4 What has happened to the data (e.g. has it been lost or stolen;
6.4.5 Whether the data could be put to any illegal or inappropriate use;
6.4.6 Data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
6.4.7 Whether there are wider consequences to the breach.

7. Notification

7.1 The IO and or the HRD, in consultation with relevant managers and or BoD member will establish whether the Information Commissioner's Office (ICO) will need to be notified of the breach, and if so, to notify them within 72 hours (where feasible) of becoming aware of the breach.

7.2 Every breach will be assessed on a case by case basis; however, the following will always be considered:

7.2.1 Whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Privacy laws;

7.2.2 Whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);

7.2.3 Whether notification would help prevent the unauthorised or unlawful use of personal data;

7.2.4 Whether there are any legal and or contractual notification requirements;

7.2.5 The dangers of over notifying. Not every breach needs to be notified, over notification may cause disproportionate enquiries and unnecessary work.

7.3 Individuals whose personal data has been affected by the breach, (and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms), will be informed of the breach without undue delay.

Notification will include a description of how and when the breach occurred and the data involved.

Specific and clear advice will be given on what the data subject can do to protect themselves, and include what action has already been taken to mitigate the risks.

Individuals will also be provided with a way in which they can contact LCL Awards for further information or to ask questions on what has occurred.

7.4 The IO and or the HRD with the authority of a BoD member must consider notifying third parties such as the police, insurers, banks or credit card companies of the breach.

This would be 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.

7.5 The IO and or the HRD with a BoD member will consider whether a press release is required to be published and to be ready to handle any incoming press enquiries.

7.6 A record will be kept of any personal data breach, regardless of whether notification was required.

8. Evaluation and response

8.1 Once the initial incident is contained, the HRD 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.

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

8.3 The review will consider:

8.3.1 Where and how personal data is held and where and how it is stored;

8.3.2 Where the biggest risks lie including identifying potential weak points within existing security measures;

8.3.3 Whether methods of transmission are secure; sharing minimum amount of data necessary;

8.3.4 The levels of staff awareness;

8.3.5 Implementing a data breach plan and identifying individuals responsible for reacting to reported breaches of security.

8.4 If deemed necessary, a report recommending any changes to systems, policies and procedures will be prepared for consideration by the BoD.

9. Policy Review

9.1 This policy will be updated as necessary to reflect best practice, changes to regulation and or legislation to ensure continuing compliance.

9.2 This policy was written in May 2018. The policy was approved by the BoD in May 2018.