General Data Protection Regulation (GDPR) Policy and Process

Table of Contents

Introduction

Data Security Breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. CIOL Qualifications (CIOLQ) is duty bound to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation of the European Parliament, the Council of the European Union and the European Commission intended to strengthen and unify data protection for all individuals within the European Union (EU). It requires that all organisations publish and maintain a policy on data protection and how personal data is handled.

Scope

This company-wide policy applies to all CIOL Qualifications information, regardless of format, and is applicable to all staff and stakeholders associated with the CIOLQ and data processors acting on behalf of the CIOLQ. It is to be read by all members of staff and 3rd parties who have access to CIOLQ data.

Aim

The aim of this policy is to standardise the CIOLQ response to any reported data breach incident and ensure that they are appropriately logged and managed in accordance with best practice guidelines.

By adopting a standardised consistent approach to all reported incidents, it aims to ensure that:

- Incidents are reported in a timely manner and can be properly investigated
- Incidents are handled by authorised personnel
- Appropriate levels of CIOLQ executives & management are involved in incidents and responses
- Incidents are recorded and documented
- The impact of incidents are understood and action is taken to prevent further damage
- Evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- External bodies or data subjects are informed as required
- The incidents are dealt with in a timely manner and normal operations restored
- The incidents are reviewed to identify improvements in policies and procedures.

Definition of data breach

A data security breach is considered to be “any loss of, or unauthorised access to CIOL Qualifications data”.

Examples of data security breaches may include:

- Loss or theft of data or equipment on which data is stored
- Unauthorised access to confidential or highly confidential CIOLQ data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood

- Hacking attack
- Data 'blagging' offences where information is obtained by deceit
- Sharing of candidate data to unathorised third parties

CIOLQ Virtual Centre data requirement

Recording of exams

Exam sessions will be video recording for marking and quality assurance purposes. No such recordings will be shared other than for invigilation, internal CIOLQ processing or regulatory purposes, without candidate consent.

CIOLQ will seek to protect that privacy of candidates arising from this monitoring, recording and filming during your exam. Without being able to record and film candidates during live invigilation we would not be able to assess you.

Candidate identification

At the start of each exam session, all candidates will be required to show a valid photographic ID and verify their signature using the web camera facility for identification purposes. Exam sessions will not commence if we are not able to verify a candidate's identity.

Accepted forms of photographic ID:

- Passport
- National ID card
- Driving licence

Candidate consent

Showing your photographic ID prior to the exam taking place will be taken as your consent to being monitored, recorded and filmed for the purposes of your exam as well as for playback after the exam for marking, moderation as well as for referring to in the event of an appeal, complaint or special consideration.

GDPR Data Controllers and Data Processors

The GDPR draws a distinction between a 'controller' and a 'processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility.

The GDPR defines these terms:

- 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

If you are a controller, you are responsible for complying with the GDPR – you must be able to demonstrate compliance with the data protection principles and take appropriate technical and organisational measures to ensure your responsibilities are carried out in line with the GDPR. If you are a processor, you have more limited compliance responsibilities.

Responsibility

- CIOLQ staff, associates and 3rd parties who have access to data are responsible for reporting actual, suspected, threatened or potential information security breach incidents and for assisting with investigations as required; particularly if urgent action must be taken to prevent further damage.
- Departmental Heads are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.
- The GDPR data team will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Suitable delegation may be appropriate in some circumstances.

Data Classification

Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore, it is important to identify quickly, the classification of the data and respond to all reported incidents in a timely and thorough manner.

All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted.

The severity and risk associated with a data breach can be found in **Appendix C: Evaluation of Incident Severity**

Data Security Breach Reporting

External identification

Confirmed or suspected data security breaches should be reported promptly to CIOLQ Head of Qualifications +44 020 7940 3100 or email qualifications@ciol.org.uk The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. Where possible the incident report form should be completed as part of the reporting process.

Once a data breach has been reported an initial assessment will be made to establish the severity of the breach and who the responsible officer to lead should be.

All data security breaches will be centrally logged on the data breach document to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

Internal identification

As External identification with regard to the initial assessment and severity rating. Whether the identification is actual or potential the staff identifier must report it immediately to their line manager who will escalate it to the Responsible Officer.

Data Breach Management Plan

The response to any reported data security breach will involve the following four elements:

See Appendix A

1. Containment and Recovery
2. Assessment of Risks
3. Notification
4. Review and Response

Each of the four elements will need to be conducted in accordance with the checklist for Data Security Breaches.

An example of an activity log spreadsheet is attached (D).

Appendix B: Data Breach Incident Report Form
Appendix C: Evaluation of Incident Severity and Checklist
Appendix D: Example format of timeline of breach

Authority & Disciplinary Procedures

CIOL Qualifications staff, associates and 3rd parties who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

Review

The GDPR data team will monitor the effectiveness of this policy and carry out regular reviews of all reported breaches.

References

ICO website: guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Policy updating and reviewing

All policies relating to CIOLQ will be updated on an 18-month cycle or sooner as required.

Policy version and owner

Policy review date	November 2024
Policy owner	Responsible Officer

Appendix A: Data Breach Management Plan

Containment and Recovery

- Department Manager to be notified and assign severity of the breach using appendix 2
- Forward copy of the completed data breach form to relevant passes
- Identify the cause of the breach and if it has been contained or is ongoing, ensure that any further potential for data loss is either protected, removed or is mitigated as much as possible
- Determine if anything can be done to recover the loss of data and limit any damage
- Where appropriate notify the relevant external authorities
- Ensure all key actions are logged and decisions recorded

Assessment of risks

- What type of data and how much is involved?
- How sensitive is the data?
- What has happened to the data?
- If the data was lost or stolen were there any protections in place to prevent access or misuse e.g. encryption?
- What could the data tell a third party about the individual and how this could be misused?
- Is there actual or potential harm that could come to any individuals?
- Are there wide consequences to consider (media or loss of confidence in CIOLQ)?
- Are there others who might advise of risks (e.g. banks or government authorities)?

Notification

- Are there any legal, contractual or regulatory requirements to notifying?
- Can notification help the individual?
- If a large number of people are affected or there are very serious consequences, inform the ICO
- Consider the dangers of 'over notifying' due to the impact of disproportionate enquires and work impact other areas of the data breach
- Consider how you will notify those impacted
    - Consider the urgency of the situation and impact
    - Description of the breach and what data was lost
        - Give specific and clear advice on ways to protect themselves
        - Provide ways individuals can be contact CIOLQ for more information
- Consult ICO guidance on when and how to notify it about breaches
- Consider notifying third parties who can assist or mitigating impact on individuals (police, insurers, banks etc.)

Review and Response

- Establish if there are any present or future risks
- Consider the data and context of the breach
- Consider and identify any weak points in existing security measures and procedures, with a view to changing processes or training of CIOLQ staff
- Report on findings and outcomes to Senior management and implement agreed changes

Appendix B: Data Breach Incident Report Form – for CIOL Qualifications

Person initially reporting the breach: (Name, Department, Country)	
Time and date breach was identified and by whom:	
Description of the Data Breach:	
Contact details of person reporting breach:	
Type and Severity of Breach (system and who it affects):	
Volume of data involved:	
Confirmed or suspected breach: Confirmed: Y/N *Provide further details:*	
Is the breach ongoing?	
If ongoing, what actions are being taken to resolve the data, mitigate the risk?	
Who has been informed of the breach so far?	
Has the breach been rectified? Provide details:	
Does the Data Breach need reporting to Regulatory Authorities (e.g. Ofqual, Qualifications Wales, ICO)?	
Any other relevant information:	

Please email the completed form to the data team: qualifications@ciol.org.uk

For office use only

Received by:	
Date/Time:	

Appendix C: Evaluation of Incident Severity and Checklist

The severity of the incident will need to be assessed and the relevant members of the CIOLQ team notified, the assessment should be based upon the following criteria:

Critical level	Main contact
Highly Critical: Major Incident	
• Highly Confidential /Confidential Data (including financial information) • Personal identifiable data breach of over 1000 individuals • External third-party data involved • Significant or irreversible consequences • Likely media coverage • Immediate response required regardless of whether it is contained or not • Requires significant response from one or more teams	• A member of the GDPR data team • Chair of Board, CEO, Marketing Manager and Manager responsible for the area that has breached • Department Head who is responsible for the area that has breached • Other relevant contacts • ICO or Police
Moderately Critical: Serious Incident	
• Confidential Data • Not contained within CIOLQ • Breach involves personal data of more than 100 individuals but less than 1000 • Incident may not yet be contained • Incident does not require immediate response • Incident response may require notification to CIOL's CEO	• A member of the GDPR data team • Chair of Board, CEO, Marketing Manager • Department Head who is responsible for the area that has breached • Other relevant contacts • ICO or Police
Low Critical: Minor Incident	
• Internal or Confidential Data • Small number of individuals involved • Risk to CIOLQ low • Inconvenience may be suffered by individuals impacted • Loss of data is contained/encrypted • Incident can be responded to during working hours Example – Email sent to wrong person, loss of data is encrypted	• A member of the GDPR data team • Department Head who is responsible for the area that has breached • CEO and Marketing Manager and the Manager responsible for the area that has breached

Appendix D: Example Format of Timeline of Breach

Actual format is a spreadsheet log stored on the shared drive

Date	Time	Activity	Decision	Authority	Date Authorised