

General Data Protection Regulation (GDPR) Policy and Process

Table of Contents

Introduction..... 3

Scope 3

Aim 3

Definition of data breach 3

CIOLQ Virtual Centre data requirement 4

GDPR Data Controllers and Data Processors 4

Responsibility 4

Data Classification 5

Data Security Breach Reporting 5

Data Breach Management Stages 6

Authority & Disciplinary Procedures..... 6

Review 6

References..... 6

Policy updating and reviewing 6

Policy version and owner 6

Appendix A: Data Breach Management Plan..... 7

Appendix B: Data Breach Incident Report Form – for CIOLQ 8

Appendix C: Evaluation of Incident Severity and Checklist..... 9

Appendix D: Breach Timeline (sample format) 10

Introduction

Data Security Breaches are increasingly common occurrences whether these are caused by human error or via malicious intent. As technology trends change and the volume of created data and information increases, 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 wherever possible.

The handling of personal data in the UK is governed by the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the Data (Use and Access) Act 2025 (DUAA 2025). Following the UK's exit from the European Union, the EU's General Data Protection Regulation (Regulation (EU) 2016/679) was transposed into UK national law as the UK GDPR, with technical amendments made under the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. The DPA 2018 supplements the UK GDPR by providing for exemptions and derogations under UK law. The DUAA 2025, which came substantially into force in February 2026, introduced further updates including recognised legitimate interests for data processing and reforms to automated decision-making rules. Together, these instruments require organisations to maintain and publish a clear policy on data protection and the handling of personal data.

Scope

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

Aim

The aim of this policy is to standardise CIOLQ's response to any reported data breach incident, and to ensure that such an occurrence is appropriately logged and managed in accordance with best practice guidelines.

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

- Incidents are reported promptly 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 is 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 promptly 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
- An incidence of hacking or data compromise, such as a Ransomware attack
- Data 'blagging' offences where information is obtained by deceit (also referred to as Spear Phishing)
- Any other general phishing attempt, mass or otherwise
- Sharing of candidate data with unauthorised third parties

CIOLQ Virtual Centre data requirement

Recording of exams

Both video and audio recording will take place during all exam sessions, for marking and quality assurance purposes. No such recordings will be shared other than for invigilation, internal CIOLQ processing, or regulatory purposes, without the candidate's consent.

CIOLQ will seek to protect the privacy of candidates arising from this monitoring, recording, and filming during an exam. Without being able to record and film candidates during live invigilation we would not be able to adequately assess performance, moderate an exam session if required, or appropriately respond to post-exam queries.

Candidate identification

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

Accepted forms of photographic ID:

- Passport
- National ID card
- Full Driving licence (a provisional licence will not be accepted)

Candidate consent

Showing photographic ID at the start of any exam will be taken as consent regarding the monitoring, recording and filming of said exam, for the purposes of invigilation, post-exam marking, moderation and internal training, alongside reference purposes in the event of an appeal, complaint, or request for 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 as:

- '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 third 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 the 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 the classification of any data involved, and respond to any and all reported incidents, in both a timely and thorough manner.

All reported incidents will need to include the appropriate data classification in order for the 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 and Checklist**.

Data Security Breach Reporting

External identification

Confirmed or suspected data security breaches should be reported promptly to CIOLQ's Head of Qualifications via the following means:

- Tel: +44 020 7940 3100
- Email: qualifications@ciol.org.uk

The report should include full and accurate details of the incident, including (but not limited to):

- Who is reporting the incident
- What classification of data is involved

Where possible, as part of the reporting process use **Appendix B: Data Breach Incident Report Form – for CIOLQ**.

Once a data breach has been reported, an initial assessment will be made to establish both the severity of the breach and who the responsible officer to lead on the incident should be, using **Appendix C: Evaluation of Incident Severity and Checklist**.

All data security breaches will be centrally logged to ensure appropriate oversight of the types and frequency of confirmed incidents for management and reporting purposes. The actual format is a spreadsheet log stored on the CIOLQ shared drive. **Appendix D: Breach Timeline (sample format)** is an example of the type of information logged.

Internal identification

Whether the identification is actual or potential, the identifying staff member must report it immediately to their line manager, who will escalate it to the Responsible Officer.

Data Breach Management Stages

The response to any reported data security breach will involve the following four management stages.

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

Each of the stages will need to be considered following **Appendix A: Data Breach Management Plan**.

Authority & Disciplinary Procedures

CIOLQ staff, associates and third 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: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>

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 2027
Policy owner	Responsible Officer

Appendix A: Data Breach Management Plan

Stage 1 - Containment and Recovery

- The Department Manager is to be notified and assign the severity of the breach using **Appendix C: Evaluation of Incident Severity and Checklist**
- Forward a copy of the completed data breach form to all relevant parties
- 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 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

Stage 2 - 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 could this be misused?
- Is there actual or potential harm that could come to any individual(s)?
- Are there wider consequences to consider (media exposure or loss of confidence in CIOLQ)?
- Are there other parties to advise of risks (e.g. banks or government authorities)?

Stage 3 - Notification

- Are there any legal, contractual, or regulatory notification requirements that need to be adhered to?
- Can notification help the individual?
- If a large number of people are affected or there are very serious consequences, inform the ICO
- Consider the risk of 'over notifying' and the impact a high volume of enquiries could have on workload in other areas of the organisation impacted by the data breach
- Consider how you will notify those impacted:
 - Consider the urgency of the situation and its impact
 - Description of the breach and what data was lost
 - Give specific and clear advice on ways to protect themselves
 - Provide ways individuals can 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 mitigate the impact on individuals (police, insurers, banks, etc.)

Stage 4 - Review and Response

- Establish if there are any present or future risks
- Consider the data involved in, and/or 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 CIOLQ

The 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 the person reporting the breach:	
Type and Severity of Breach (system and who it affects):	
The volume of data involved:	
Confirmed or suspected breach: Confirmed: Y/N <i>Provide further details:</i>	
Is the breach ongoing?	
If ongoing, what actions are being taken to resolve the issue, and 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: 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 relevant staff in the CIOLQ team notified. The assessment should be based on the following criteria:

Critical level	Main contact
Highly Critical: Major Incident	
<ul style="list-style-type: none"> • 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 is required regardless of whether it is contained or not • Requires significant response from one or more teams 	<ul style="list-style-type: none"> • A member of the GDPR data team • Chair of Board, CEO, Marketing Manager, and Manager responsible for the area that has been breached • Department Head who is responsible for the area that has been breached • Other relevant contacts • ICO or Police
Moderately Critical: Serious Incident	
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • A member of the GDPR data team • Chair of Board, CEO, Marketing Manager • Department Head who is responsible for the area that has been breached • Other relevant contacts • ICO or Police
Low Critical: Minor Incident	
<ul style="list-style-type: none"> • 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 <p>Example – Email sent to the wrong person, loss of data is encrypted</p>	<ul style="list-style-type: none"> • A member of the GDPR data team • Department Head who is responsible for the area that has been breached • CEO, Marketing Manager and Manager responsible for the area that has been breached

Appendix D: Breach Timeline (sample format)

The actual format is a spreadsheet log stored on the CIOLQ shared drive

Date	Time	Activity	Decision	Authority	Date Authorised