

Quest for Learning Data Breach Procedure

Document control:

Version	August 2026
Review date	August 2028
Owner	Chief Executive
Operational lead	Data Protection Lead
Approved by	Chief Executive
Governance level	Level 2 - Procedure
Document reference	PRO-DP-001

Quest for Learning Governance Framework

This document forms part of Quest for Learning's Governance Framework.

Level 1 – Policies

Policies define the Charity's principles, governance arrangements, responsibilities and organisational expectations.

Level 2 – Procedures & Guidance

Procedures and guidance explain how policies are implemented in practice.

Level 3 – Forms, Registers & Templates

Forms, registers and templates provide the records and evidence required to demonstrate compliance.

1. Purpose

Quest for Learning is committed to protecting the personal information entrusted to it and responding promptly and effectively whenever an actual or suspected data breach occurs.

This procedure explains how personal data breaches must be:

- recognised;
- reported;
- contained;
- assessed;
- investigated;
- recorded;
- notified where required;
- reviewed to identify lessons and prevent recurrence.

The procedure is intended to ensure that incidents are managed consistently, proportionately and in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018 and the Charity's Information Governance and Data Protection Policy.

Some personal data breaches must be reported to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of the Charity becoming aware of them. It is therefore essential that all actual or suspected breaches are reported internally immediately, even where they appear minor or have already been contained. ([ICO](#))

2. Scope

This procedure applies to:

- Trustees;
- employees;
- freelance tutors;
- volunteers;
- contractors;
- consultants;
- agency workers;
- any other person handling personal information on behalf of Quest for Learning.

It applies to personal information held or communicated:

- electronically;
- on paper;
- verbally;
- through photographs, video or audio recordings;
- on portable devices or storage media;
- within cloud-based systems;
- by third-party processors acting on behalf of the Charity.

This procedure applies whether an incident occurs:

- within the Charity's office;
- in a school or partner organisation;
- while working remotely;
- while travelling;
- through a third-party system or service provider.

3. What is a personal data breach?

A personal data breach is a security incident that leads to the accidental or unlawful:

- destruction;
- loss;
- alteration;
- unauthorised disclosure of;
- unauthorised access to personal information.

A breach does not need to involve deliberate wrongdoing or a cyberattack. Accidental errors, lost information, inappropriate access and failures of availability may also constitute personal data breaches.

Personal data breaches may affect the:

Confidentiality of information

Information is accessed or disclosed to someone who is not authorised to receive it.

Examples include:

- an email containing pupil information sent to the wrong recipient;
- confidential documents left where others can see them;
- a member of staff accessing records without a legitimate reason;
- recipients' email addresses disclosed by using the "To" or "Cc" field instead of "Bcc";
- personal information discussed where an unauthorised person can overhear it.

Integrity of information

Information is altered, corrupted or changed without proper authorisation.

Examples include:

- pupil assessment data being changed incorrectly;
- records being overwritten or corrupted;
- inaccurate information being entered into a system and relied upon;
- files being maliciously or accidentally modified.

Availability of information

Information is lost, destroyed or made unavailable when it is required.

Examples include:

- loss of paper pupil records;
- accidental deletion of records without an available backup;
- ransomware or another cyber incident preventing access to systems;
- loss or theft of a laptop, telephone or storage device containing personal information.

A security incident involving organisational information but no personal information may not be a personal data breach under UK GDPR. It should nevertheless be reported where it presents a security, safeguarding, operational or reputational risk.

4. Examples relevant to Quest for Learning

Examples of incidents that must be reported include:

- pupil information sent to the wrong school, parent, tutor or funder;
- a tutor losing assessment records, teaching notes or attendance information;
- a device containing QfL information being lost or stolen;
- confidential information being stored on an unauthorised personal device or account;
- unauthorised access to the Charity's information management system;
- an account being compromised through phishing or disclosure of a password;
- sensitive information about a child being overheard or seen by an unauthorised person;
- personal information being shared with a partner organisation without an appropriate basis;
- paper records being placed in ordinary waste rather than confidential disposal;
- information being accidentally published on the website;
- a supplier or cloud-service provider notifying QfL of a security incident;
- personal information being deleted, corrupted or made inaccessible;
- an email containing personal information being forwarded outside the Charity without authorisation;
- a former staff member retaining access to QfL systems;
- a near miss where a breach was narrowly avoided.

This list is not exhaustive.

Individuals must not attempt to decide for themselves that an incident is too insignificant to report. The Data Protection Lead is responsible for determining

whether the incident constitutes a personal data breach and what further action is required.

5. Roles and responsibilities

5.1 Everyone working on behalf of Quest for Learning

Anyone who becomes aware of an actual or suspected data breach must:

- report it immediately;
- take reasonable and safe steps to limit further disclosure or loss;
- preserve relevant evidence;
- provide accurate information about what occurred;
- cooperate with any investigation;
- maintain confidentiality while the incident is being managed.

Individuals must not:

- conceal or delay reporting an incident;
- delete relevant messages, files or records;
- contact the Information Commissioner's Office directly unless authorised;
- contact affected individuals unless instructed to do so;
- make admissions of liability or speculate about the likely consequences;
- attempt technical remediation beyond their knowledge or authority.

Good-faith reporting will be encouraged. The focus will be on containing the incident, protecting individuals and learning from what occurred rather than assigning blame prematurely.

5.2 Managers

Managers must:

- ensure that incidents reported to them are escalated immediately to the Data Protection Lead;
- support containment and fact-finding;
- ensure relevant records and evidence are preserved;
- make staff available to assist with the investigation;
- implement remedial actions within their area of responsibility.

A manager receiving a report must not delay escalation while attempting to investigate the incident personally.

5.3 Data Protection Lead

The Data Protection Lead is responsible for coordinating the Charity's response.

This includes:

- opening and maintaining the breach record;
- confirming when the Charity became aware of the breach;
- coordinating containment and recovery;
- assessing the likelihood and severity of harm to individuals;
- determining whether external notification is required;
- preparing recommendations for the Chief Executive;
- coordinating communication with affected individuals where necessary;
- maintaining evidence of decisions and actions;
- overseeing investigation and lessons learned.

5.4 Chief Executive

The Chief Executive has overall responsibility for the Charity's response and normally authorises:

- notification to the Information Commissioner's Office;
- communication with affected individuals;
- notification to Trustees, insurers, commissioners, schools, funders or other external organisations;
- significant remedial action;
- escalation under the Charity's Risk Management or Business Continuity arrangements.

Where the Chief Executive is unavailable and delay could prevent the Charity from meeting its legal obligations, the Data Protection Lead may take necessary action within their delegated authority and inform the Chief Executive as soon as possible.

5.5 Board of Trustees

The Board should be informed where a breach:

- presents a significant risk to individuals or the Charity;
- is reported to the ICO;
- involves a substantial safeguarding, legal, financial, operational or reputational risk;
- indicates a serious or systemic control weakness;
- requires significant organisational action or expenditure.

The Board's role is to provide oversight and assurance rather than manage the operational response.

6. Immediate action by the person discovering the incident

Anyone who discovers or suspects a breach must follow the steps below. (NB a Data Breach Immediate Action Guide is also available in the Policies folder – document reference GUI-DP-001).

Step 1: Act immediately to prevent further harm

Where safe and reasonably possible:

- recall or withdraw an incorrectly sent email;
- ask an unintended recipient not to open the information and to delete it securely;
- retrieve paper records left in an insecure location;
- disconnect a compromised device from the network without deleting evidence;
- lock or remotely disable a lost device where authorised;
- change a compromised password;
- stop further distribution or publication of the information;
- preserve any relevant emails, screenshots, system messages or documents.

Containment action must not delay reporting.

Step 2: Report the incident immediately

The incident must be reported to the Data Protection Lead and the individual's manager as soon as it is discovered.

Where the Data Protection Lead is unavailable, it must be reported to the Chief Executive.

The report should be made using the quickest available secure method. The Data Breach Report Form should then be completed as soon as practicable.

Step 3: Provide the available facts

The initial report should include, where known:

- the date and time the incident occurred;
- the date and time it was discovered;
- who discovered it;
- what happened;
- the type of information involved;
- whose information may be affected;

- approximately how many people and records may be involved;
- who may have received or accessed the information;
- whether the information has been recovered, deleted or secured;
- any immediate action already taken;
- whether children or vulnerable individuals may be affected;
- whether the incident is continuing.

A report must not be delayed because some information is not yet known.

Step 4: Preserve evidence and await instructions

The individual must:

- keep all relevant records;
- avoid deleting emails or files;
- retain envelopes, devices or documents where relevant;
- make notes while events remain fresh;
- follow instructions from the Data Protection Lead.

The 72-hour reporting period runs from when the Charity becomes aware that a personal data breach has occurred, not from when the underlying incident originally happened. The Charity should therefore begin logging and assessing an incident immediately, even where further investigation is required. ([ICO](#))

7. Initial triage by the Data Protection Lead

On receiving a report, the Data Protection Lead should immediately:

1. record the date and time the report was received;
2. establish whether personal information is involved;
3. determine whether the incident is continuing;
4. coordinate urgent containment;
5. identify the systems, locations and organisations involved;
6. establish whether a processor or partner must be contacted;
7. assess whether specialist IT, safeguarding, legal or insurance advice is required;
8. begin the breach assessment;
9. establish the deadline by which any ICO notification must be made.

Where it is not yet clear whether a personal data breach has occurred, the incident should still be logged and investigated promptly.

All confirmed personal data breaches must be recorded, including those that are assessed as not requiring notification to the ICO. The record should document what happened, the effects of the breach, the risk assessment, the decision reached and the remedial action taken. ([ICO](#))

8. Containment and recovery

The immediate priority following any actual or suspected personal data breach is to limit further loss, disclosure, alteration or unavailability of information and to reduce the potential impact on affected individuals.

Containment action should begin as soon as possible and must not be delayed while the full circumstances are investigated.

8.1 Containment

The Data Protection Lead will coordinate proportionate containment action, working with the Chief Executive, relevant managers, IT providers, schools, partners or third-party processors as necessary.

Depending on the nature of the incident, containment measures may include:

- recalling or withdrawing an incorrectly sent email;
- contacting an unintended recipient and requesting secure deletion or return of information;
- obtaining written confirmation that information has not been copied, retained or shared;
- recovering misplaced paper records;
- suspending or restricting access to systems or accounts;
- resetting passwords or authentication credentials;
- remotely locking or wiping lost or stolen devices;
- disconnecting affected equipment from networks;
- removing information published or shared in error;
- suspending a compromised process or service;
- instructing a third-party processor to take urgent remedial action;
- preserving system logs, emails, documents and other evidence.

Where an incident involves a school, partner organisation, supplier or processor, responsibilities for containment should be agreed promptly and clearly recorded.

Where Quest for Learning is acting as a processor on behalf of another organisation, the relevant controller must be informed without undue delay in accordance with the applicable contractual arrangements.

8.2 Recovery

Once the immediate incident has been contained, the Charity will consider what action is required to restore the security, accuracy and availability of affected information and services.

Recovery measures may include:

- restoring information from secure backups;
- checking the integrity and accuracy of recovered records;
- correcting or replacing altered information;
- reinstating systems only after appropriate security checks;
- reviewing user access permissions;
- monitoring accounts or systems for further unauthorised activity;
- providing alternative arrangements while systems remain unavailable;
- supporting affected staff, tutors, schools or individuals;
- obtaining specialist technical, legal, safeguarding or insurance advice.

Systems or processes should not return to normal operation until the Charity is reasonably satisfied that the immediate threat has been addressed and that doing so will not create further risk.

8.3 Recording containment and recovery

All material containment and recovery actions must be recorded within the breach record, including:

- what action was taken;
- when it was taken;
- who authorised or completed it;
- whether it was successful;
- any evidence obtained;
- any risks that remain.

Containment does not automatically mean that a breach is no longer reportable. The risk assessment must consider the consequences of the breach after taking account of any effective mitigation. ([ICO](#))

9. Assessing risk to individuals

Every confirmed personal data breach must be assessed to determine the likelihood and severity of harm to the rights and freedoms of the people affected.

The assessment must focus primarily on the possible consequences for individuals rather than solely on the operational, financial or reputational consequences for Quest for Learning.

The assessment should be completed as promptly as possible and reviewed as further facts become available.

9.1 Potential harm

Personal data breaches may result in physical, material or non-material harm.

Possible consequences include:

- loss of confidentiality;
- distress, anxiety or embarrassment;
- discrimination or stigma;
- identity theft or fraud;
- financial loss;
- damage to reputation;
- loss of control over personal information;
- safeguarding risks;
- physical danger;
- misuse of contact or location information;
- loss of access to services or opportunities;
- harm to family, educational or professional relationships.

The absence of proven harm at the time of assessment does not necessarily mean that no risk exists.

9.2 Factors to consider

The Data Protection Lead should consider:

The nature of the information

- whether the information directly identifies individuals;
- whether it includes special category or criminal offence data;
- whether it includes safeguarding, health, disability or SEND information;
- whether it includes financial, identity, login or contact details;
- whether separate pieces of information could be combined to identify or harm someone;
- whether the information was encrypted, pseudonymised or otherwise protected.

The people affected

- whether children are involved;
- whether individuals may be vulnerable because of age, disability, personal circumstances or safeguarding concerns;
- whether the breach could place an individual at risk from another person;
- whether the affected individuals may have particular reasons to expect confidentiality;
- the number of individuals involved.

Because Quest for Learning regularly processes information relating to children, the potential vulnerability of affected individuals must be given particular weight.

The circumstances of the breach

- whether the breach was accidental or deliberate;
- who received or may have accessed the information;
- whether the recipient is known and trusted;
- whether the information has been copied, forwarded or published;
- whether there is evidence of malicious intent;
- how long the information was exposed or unavailable;
- whether the incident is ongoing;
- whether the information has been recovered or securely deleted;
- whether a compromised device or account was protected;
- whether containment can be independently verified.

The likely consequences

- the seriousness of any potential harm;
- how likely it is that harm will occur;
- whether any harm may be immediate or arise later;
- whether the effects could be reversed or mitigated;
- whether individuals can take practical steps to protect themselves.

The assessment should consider both the **likelihood** of harm occurring and the **severity** of the possible consequences. A breach may represent a high risk because serious harm is likely, because the potential harm would be particularly severe, or through a combination of both. ([ICO](#))

9.3 Risk outcome

The assessment should reach one of the following conclusions.

Where the outcome is uncertain, the Charity should adopt a cautious approach, consult current ICO guidance and obtain specialist advice where appropriate.

Unlikely to result in a risk The breach is unlikely to affect the rights and freedoms of individuals. The ICO does not normally need to be notified, but the breach and the reasons for the decision must still be recorded.	Likely to result in a risk There is a realistic likelihood of adverse consequences for affected individuals. The ICO must be notified without undue delay and, where feasible, within 72 hours of the Charity becoming aware of the breach.
Likely to result in a high risk The likelihood or potential severity of harm is sufficiently significant to meet the higher threshold. The ICO must be notified and affected individuals must normally also be informed without undue delay.	

10. Deciding whether to notify the Information Commissioner's Office

Quest for Learning must notify the Information Commissioner's Office where a personal data breach is likely to result in a risk to the rights and freedoms of individuals.

Not every personal data breach requires notification. Where the breach is unlikely to result in such a risk, the Charity may decide not to report it, provided that the assessment and reasons are fully documented. ([ICO](#))

10.1 Authority to notify

The Chief Executive will normally authorise notification to the ICO following advice from the Data Protection Lead.

Where the Chief Executive is unavailable and delay could cause the Charity to miss the statutory reporting period, the Data Protection Lead may make or authorise the notification and inform the Chief Executive as soon as possible.

10.2 Reporting timescale

Where notification is required, it must be made:

- without undue delay; and
- where feasible, within 72 hours of the Charity becoming aware of the breach.

The 72-hour period continues to run outside normal working hours, including weekends and bank holidays.

If notification is made after 72 hours, the Charity must explain the reasons for the delay.

The Charity should not postpone notification solely because every detail has not yet been established. An initial notification may be made using the information available, with further information supplied in phases where necessary.

10.3 Information included in the notification

The notification should include, where available:

- a description of the nature of the breach;
- the categories and approximate number of individuals affected;
- the categories and approximate number of records affected;
- the name and contact details of the Data Protection Lead or other contact point;
- the likely consequences of the breach;
- the action taken or proposed to contain and mitigate it;
- the reasons for any delay in reporting;
- any other information reasonably requested by the ICO.

The Charity must retain a copy of the notification and any subsequent correspondence.

10.4 Decision not to notify

Where the Charity decides that ICO notification is not required, the breach record must clearly document:

- the facts known at the time;
- the risk assessment undertaken;
- the mitigation and containment achieved;
- why harm to individuals was considered unlikely;
- who made and authorised the decision;
- any advice obtained.

The decision should be reviewed if new information later indicates that the risk is greater than originally assessed.

10.5 Seeking advice

Where the reporting threshold is unclear, the Data Protection Lead may:

- use the ICO's current breach self-assessment resources;
- contact the ICO for advice;
- seek specialist legal, technical, safeguarding or insurance advice.

Seeking advice does not pause the 72-hour period. ([ICO](#))

11. Informing affected individuals

Where a personal data breach is likely to result in a **high risk** to the rights and freedoms of individuals, Quest for Learning must normally inform those individuals directly and without undue delay.

The purpose of communication is to enable people to understand what has happened, take appropriate precautions and obtain support where necessary. ([ICO](#))

11.1 Authority and coordination

Communication with affected individuals will normally be authorised by the Chief Executive and coordinated by the Data Protection Lead.

Where children are affected, the Charity will carefully consider whether communication should be directed to:

- the child;
- their parent or carer;
- the relevant school;
- another person with parental responsibility;
- a combination of these parties.

The approach must reflect the child's age and understanding, the nature of the information, safeguarding considerations, existing contractual or data-sharing arrangements and the need to avoid creating further risk.

Safeguarding advice should be sought where notifying a parent, carer or another person could itself place a child or individual at risk.

11.2 Content of the communication

The communication should be clear, concise and written in accessible language.

It should normally explain:

- what happened;
- when the breach occurred and was discovered;
- what information was involved;
- the likely consequences;
- what Quest for Learning has done to contain and investigate the breach;
- what further action the Charity intends to take;
- practical steps the individual can take to protect themselves;
- where they can obtain further information or support;
- how to contact Quest for Learning;
- their right to raise a concern with the ICO.

The communication should avoid:

- unnecessary technical language;
- speculation;
- misleading reassurance;
- disclosing personal information about other affected people;
- making admissions of legal liability without appropriate advice.

11.3 Method of communication

Affected individuals should normally be contacted directly using an appropriate and secure method, such as:

- telephone;
- secure email;
- letter;
- communication through a school or partner where this is appropriate and agreed.

The method chosen should reflect:

- the urgency of the situation;
- the sensitivity of the information;
- the number and needs of those affected;
- whether the normal communication channel may itself have been compromised;
- accessibility and safeguarding requirements.

Where direct communication would involve disproportionate effort, the Charity will seek appropriate advice before using broader public communication.

11.4 When communication may not be required

Direct communication may not be necessary where:

- effective technical and organisational protection rendered the information unintelligible to unauthorised persons;
- subsequent measures have ensured that the high risk is no longer likely to arise;
- another lawful exception applies.

Any decision not to inform affected individuals where a high-risk breach has occurred must be clearly documented and supported by appropriate advice.

The ICO may require the Charity to communicate a breach to affected individuals where it considers that the high-risk threshold has been met.

11.5 Ongoing support and updates

Where appropriate, the Charity should provide affected individuals with:

- updated information as the investigation develops;
- revised protective advice;
- a named contact point;
- reasonable support in responding to the consequences of the breach.

All communications and attempted communications must be recorded within the breach record.