Compass Learning & Education

Data Breach Procedure

Personal Data Breach Response, Notification and Recording Procedure

Policy owner	Director and Data Protection Lead - Rosie Aylward
Safeguarding adviser	Designated Safeguarding Lead
Approved by	Director - Rosie Aylward
Version	2.0
Approval date	14 July 2026
Review cycle	Annual, or sooner following a material incident, system change, contractual change or updated guidance
Date of next review	14 July 2027

1. Purpose and Scope

Compass Learning & Education will respond promptly, calmly and transparently to every actual, suspected or near-miss personal data breach. The objectives are to contain the incident, protect affected individuals, preserve evidence, assess risk, meet controller and regulatory obligations, learn from what happened and prevent recurrence.

This procedure applies to all staff, contractors, volunteers and suppliers processing personal information for Compass. It covers paper and electronic records, email, Webador-hosted business email, Outlook and connected devices, cloud systems, safeguarding and learner records, photographs, qualification data, finance, workforce information and any future approved CCTV or monitoring system.

2. Key Principles

- The safety, welfare, dignity and rights of affected individuals, particularly children and vulnerable learners, are central to decision-making.
- A breach is more than losing data; it includes loss of availability or integrity as well as unauthorised access or disclosure.
- All incidents and near misses must be reported immediately, even where the information appears low risk or has been recovered.
- Staff may take safe and proportionate containment action within their competence but must not conceal, destroy evidence or make external notifications without authorisation.
- Where Compass acts as processor, it must notify the relevant controller without undue delay. The controller decides whether it must notify the ICO, supported by information and assistance from Compass.
- Where Compass acts as controller, Compass is responsible for assessing and making any ICO and affected-person notifications.

3. Roles and Responsibilities

3.1 Director and Data Protection Lead

- receive and coordinate breach reports, containment, investigation and risk assessment;
- identify whether Compass is controller, processor or both for the affected processing;
- notify the relevant controller without undue delay where Compass acts as processor;
- decide whether Compass must notify the ICO or affected individuals where Compass acts as controller;
- maintain the breach record and central breach log, including non-reportable incidents and near misses;
- coordinate technical, legal, insurance, safeguarding and communication support;

- assign remedial actions and verify completion.

3.2 Designated Safeguarding Lead

- assess immediate safeguarding and welfare consequences;
- ensure data protection considerations do not delay action necessary to protect a child;
- advise on communication with parents, carers, schools, social care, police or other safeguarding partners;
- support decisions concerning safeguarding records and sensitive contextual information.

3.3 All Staff and Contractors

- report any actual, suspected or near-miss breach immediately by phone or in person to the Data Protection Lead;
- take safe immediate containment action where possible, such as retrieving paperwork, recalling an email or locking a device;
- preserve evidence and provide a complete and honest account;
- not delete messages, alter records, contact the ICO, media, affected people or other third parties unless authorised;
- cooperate with investigation and remedial action.

3.4 IT, System Providers and Other Suppliers

Providers must comply with their contractual incident and breach-notification obligations, preserve relevant logs and evidence, assist containment and provide information about systems, data, affected individuals, locations, subprocessors and remedial action. The Data Protection Lead will notify the relevant controller of a supplier breach affecting controller data without undue delay.

4. What Is a Personal Data Breach?

A personal data breach is a security incident that results in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. It may affect confidentiality, integrity or availability.

- a safeguarding file, EHCP or progress report sent to the wrong recipient;
- paperwork left in a classroom, vehicle or shared area;
- a lost, stolen or unlocked laptop, phone or storage device;
- a compromised password, phishing incident or unauthorised cloud-folder access;
- information accidentally overwritten, corrupted, encrypted by malware or made unavailable;
- photographs or learner information published without authority;
- confidential information discussed where an unauthorised person can hear it;
- a supplier informing Compass that its systems or subprocessors have been compromised;
- failure to delete or return information when required by contract or law.

5. Immediate Response and Escalation

Timing	Required action
Immediately	Report the incident to the Data Protection Lead by phone or in person. Where they cannot be reached and the risk is serious, contact the designated deputy or take proportionate containment action and record what was done.
Immediately	Contain the incident where safe: retrieve or secure records; recall or restrict an email; ask an unintended recipient not to open, copy or share the information and to confirm secure deletion; lock or remotely wipe a device; disable access; change compromised credentials; stop further disclosure.
Same day	Preserve evidence and record the known facts, including dates, systems, people, data, recipients, actions taken and any continuing risk. Do not delete relevant emails, audit logs or files.
Without undue delay	If Compass is a processor, notify the relevant controller of every actual personal data breach affecting data processed on its behalf. Follow any shorter contractual deadline and do not wait for the investigation to be complete.
Within 24 hours	The Data Protection Lead completes or updates the initial risk assessment, identifies further evidence and decides whether specialist, technical, safeguarding, insurer, police or legal support is required.
Within 72 hours where reportable	If Compass is the controller and the breach is likely to result in a risk to individuals, notify the ICO without undue delay and, where feasible, within 72 hours of awareness. Information may be provided in phases where necessary, with reasons for delay recorded.
Without undue delay where high risk	If Compass is the controller and the breach is likely to result in a high risk to individuals, inform affected individuals without undue delay unless an applicable legal exception applies or effective measures have removed the high risk.

6. Processor and Controller Notification

6.1 Where Compass Is Acting as Processor

The Data Protection Lead will notify the relevant school, academy trust, local authority or other controller without undue delay after becoming aware of a breach affecting information processed on its behalf. This applies to all actual breaches, not only those Compass believes are serious or reportable. The initial notice will not be delayed because facts are incomplete.

The notification will provide available information including:

- the nature of the breach and when it occurred and was discovered;
- categories and approximate numbers of individuals and records affected;
- types and sensitivity of information involved;
- known or likely consequences;
- containment and mitigation completed or proposed;
- the Compass contact for follow-up;
- information still being investigated and the expected update time.

Compass will assist the controller with its risk assessment, regulatory notification, communications, DPIA review and remedial action as required by the contract and law.

6.2 Where Compass Is Acting as Controller

The Data Protection Lead will determine whether the breach is likely to result in a risk to individuals. Reportable breaches will be notified to the ICO without undue delay and, where feasible, within 72 hours of awareness. The reasons for reporting or not reporting will be documented. Where high risk is likely, affected people will be informed in clear and accessible language unless an exception applies.

7. Risk Assessment

The assessment will consider the likelihood and severity of harm, including physical, emotional, safeguarding, discriminatory, reputational, financial, identity, educational and confidentiality harm. Factors include:

- the categories, sensitivity, volume and accuracy of the information;
- whether children, vulnerable individuals or people at safeguarding risk are affected;
- whether the information includes safeguarding, SEND, health, criminal-offence, financial, identity or location data;
- how easily individuals can be identified and whether data was encrypted or pseudonymised;

- the identity, trustworthiness and intentions of recipients;
- whether information was accessed, copied, further shared, recovered or securely deleted;
- the duration and geographical extent of exposure;
- possible misuse, exploitation, distress, discrimination, fraud, family conflict or physical danger;
- the effectiveness of containment and any continuing vulnerability;
- contractual, safeguarding, insurer, legal and regulatory requirements.

The assessment will be reviewed as new information becomes available. A low initial assessment does not prevent escalation if circumstances change.

8. Communication and Safeguarding

- Communications will be factual, timely, accessible and proportionate and will avoid unnecessary disclosure of additional personal information.
- Where a breach creates an immediate safeguarding or welfare risk, the DSL will take appropriate safeguarding action without waiting for the data-protection assessment to finish.
- Parents or carers will not automatically be contacted where doing so could increase risk or conflict with safeguarding advice.
- The relevant commissioner or school DSL will be involved where appropriate, but processor notification to the controller remains mandatory where controller data is affected.
- Only the Director or authorised delegate may communicate with the ICO, media or affected people about the breach.

9. Supplier and System Incidents

A notification from Webador, Microsoft, a cloud provider, learner or safeguarding system, payroll provider, awarding organisation or other supplier must be treated as a potential personal data breach. The Data Protection Lead will establish what data and systems are affected, the supplier's role, hosting and access locations, affected subprocessors, containment, recovery, notification decisions and the effect on commissioning controllers.

Relevant contracts, supplier contacts, audit logs, backups and business-continuity arrangements will be used to contain the incident and restore secure availability. Supplier performance and continued suitability will be reviewed after significant incidents.

10. Recording, Evidence and Learning

Every actual, suspected or near-miss breach will be recorded in the central Breach Log. The record must be sufficient to demonstrate the facts, effects, assessment and remedial action, including where Compass decides that ICO or individual notification is not required.

- Evidence such as emails, logs, screenshots, recipient confirmations and supplier notices will be preserved securely.
- A root-cause review will consider people, process, technology, workload, training, supplier, access and retention factors.
- Actions will have named owners and completion dates and may include training, access changes, encryption, system configuration, supplier action, reduced collection, improved templates or changes to policy and contracts.
- Serious or repeated incidents will be included in management review and the information-risk action plan.
- Learning will be communicated without inappropriate blame or disclosure of confidential details.

Appendix A - Personal Data Breach Record

Field	Record
Breach reference	
Date/time incident occurred or began	
Date/time discovered	
Date/time Data Protection Lead became aware	
Reporter and contact details	
Compass role for affected processing	Controller / Processor / Both / To be confirmed
Relevant commissioner/controller and contact	
Description and systems/locations involved	
Categories of personal information	
Special category or criminal-offence data involved	
Approximate number/categories of affected individuals	
Approximate number/categories of records	
Unauthorised recipients or access	
Immediate containment and evidence preserved	
Likelihood and severity assessment	
Potential consequences	
Controller notified - date/time/method/reference	
ICO notification decision, date and reference	
Affected-individual notification decision and method	
Police, safeguarding, insurer, legal or supplier action	
Root cause and lessons learned	
Follow-up actions, owners and completion dates	
Record closed by and date	

Appendix B - Central Breach Log Minimum Fields

- breach reference and status;
- date occurred, date discovered and date the Data Protection Lead became aware;
- brief description and affected system;
- controller/processor role and relevant controller;
- data and people affected;
- risk rating;
- controller notification date;
- ICO and affected-person notification decisions;
- root cause and action owner;
- closure date and review date.

References and Linked Documents

- UK GDPR and Data Protection Act 2018;
- Compass Learning Data Protection and Confidentiality Policy;
- Compass Learning Information Security Policy;
- Compass Learning Safeguarding and Child Protection Policy;
- Compass Learning Data Retention and Secure Disposal Policy;
- commissioner data processing agreements and supplier contracts;
- ICO - Personal data breaches: a guide: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/;
- ICO - What does it mean if you are a processor?: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-does-it-mean-if-you-are-a-processor/.