

HINDLE'S SCHOOL OF EXCELLENCE LTD

Data Breach Response Policy

*Immediate reporting, risk assessment and recovery | 2026-27***Immediate action**

All actual or suspected personal-data breaches must be reported immediately to Miss Joanne C. Hindle. Do not wait for proof, investigate independently, contact affected people or assume that somebody else has reported it.

Data controller	Hindle's School of Excellence Ltd
Incident lead / data-protection lead	Miss Joanne C. Hindle, Director
Contact	joanne@hindlesschoolofexcellence.co.uk 0161 764 2415
Approved by	Miss Joanne C. Hindle, Director
Approval / effective date	31 August 2026 / 1 September 2026
Policy period	1 September 2026 to 31 August 2027
Next review	1 September 2027
Version / status	2.0 / Approved

Hindle's School of Excellence Ltd
115 Rochdale Road, Bury, BL9 7BA
Registered with the Information Commissioner's Office

1. Purpose and objectives

This policy establishes a clear framework for identifying, reporting, containing, assessing, notifying, recovering from and learning from personal-data breaches. Its objectives are to protect learners, families, staff and others; meet legal duties; preserve safeguarding and operational continuity; and maintain an accurate record of incidents and decisions.

2. Scope

This policy applies to directors, employees, tutors, trainees, volunteers, contractors, processors and service providers handling personal data for Hindle's. It covers paper records, conversations, photographs, CCTV, email, cloud services, education and safeguarding platforms, removable media, mobile devices, backups and any other form of personal data, on site or during home, remote and off-site work.

3. Legal and policy framework

- UK General Data Protection Regulation, particularly Articles 5, 24, 32, 33 and 34.
- Data Protection Act 2018.
- Data (Use and Access) Act 2025 and commenced amendments to UK data-protection legislation.
- Privacy and Electronic Communications Regulations 2003 where communications or storage/access technologies are involved.
- Human Rights Act 1998, safeguarding legislation and common-law confidentiality.
- Current Information Commissioner's Office guidance.
- Hindle's Data Protection and UK GDPR, Confidentiality and Information Sharing, Safeguarding, CCTV, IT/security, Records Retention and Business Continuity policies.

4. Definition

A personal-data breach is a security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. It includes confidentiality, integrity and availability incidents. A breach may be deliberate or accidental and may exist even where data is later recovered or nobody appears to have viewed it.

Type	Examples
Confidentiality	Misdirected email; visible recipient list; unauthorised record access; overheard safeguarding discussion; lost paper file or unencrypted device.

Integrity	Incorrect or malicious alteration of attendance, assessment, financial, health or safeguarding information; unauthorised deletion or merging of records.
Availability	Ransomware, system outage, account lockout, accidental deletion or destruction preventing timely access to information needed for education, safeguarding or safety.

5. Examples requiring immediate reporting

- Email, message, letter, invoice or attachment sent to the wrong person.
- Lost, stolen, unattended or insecure laptop, phone, USB, notebook, file or printout.
- Phishing, suspicious login, compromised password, malware, ransomware or unauthorised account change.
- Personal data posted publicly, shared through an incorrect link or exposed by wrong permissions.
- A staff member, learner, contractor or third party accessing data without a legitimate need.
- Records destroyed, changed, corrupted or unavailable without authorisation.
- Information disclosed during a telephone call or conversation to an unverified person.
- Insecure disposal, missing CCTV footage, excessive data supplied in a rights request, or failure by a processor.

6. Roles and responsibilities

6.1 Director / incident and data-protection lead

- Take control of the response, maintain the breach log and appoint suitable support.
- Establish when Hindle's became aware, direct containment and ensure risks are assessed.
- Decide and document ICO and individual notification, consulting specialist advice where appropriate.
- Coordinate safeguarding, commissioners, insurers, police, cyber support, processors and communications.
- Authorise closure and ensure remedial action and lessons learned are completed.

6.2 IT or technical support

- Act only under authorised instruction and preserve logs and evidence.
- Contain affected systems, reset credentials, block malicious access and support safe recovery.
- Establish systems, accounts, dates, data and access affected without destroying evidence.
- Confirm eradication, restoration, monitoring and security improvements.
- Do not notify the ICO or affected people unless authorised by Hindle's.

6.3 DSL and safeguarding team

- Assess immediate child or adult safeguarding risk and act under safeguarding procedures.
- Advise on safe contact, information sharing and possible increased risk caused by notification.
- Record safeguarding concerns separately on the appropriate system. The Lead DSL is Joanne C. Hindle; additional/deputy DSLs are Julie Helm, Jade McFarlane and Aman Javed.

6.4 Managers and system owners

- Identify affected processes, users, contracts, data locations, backups and business-continuity needs.
- Ensure access changes and staff instructions are implemented promptly.
- Support accurate fact-finding and corrective action.

6.5 All staff, volunteers and contractors

- Report immediately, including near misses and uncertainty.
- Provide factual information, preserve messages/devices and follow instructions.

- Do not conceal, delete, alter, forward or discuss evidence except as authorised.
- Do not contact recipients, affected people, media, suppliers, police or regulators unless instructed, except to call emergency services where life or safety is at risk.

6.6 Processors and suppliers

Contracts must require processors to notify Hindle's without undue delay after becoming aware of a breach and provide the information and cooperation needed for compliance. Hindle's remains responsible for its own controller decisions and will not assume that a supplier has reported to the ICO on its behalf.

7. Staff reporting route

1. Stop and make the immediate situation safe without destroying evidence.
2. Contact Joanne C. Hindle immediately by the quickest secure means available. If unavailable and safeguarding risk exists, contact another DSL and continue attempts to reach the Director.
3. State what happened, when, where, which device/system/records are involved, who may be affected and action already taken.
4. Preserve the original message, envelope, device, screenshot, audit information or other evidence. Do not circulate copies unnecessarily.
5. Complete the initial breach report as soon as directed.

No blame for prompt reporting

Prompt reporting protects people and allows legal deadlines to be met. An accidental mistake reported openly will be addressed fairly. Deliberate concealment, misuse or failure to follow reasonable instructions may be treated as misconduct.

8. Response priorities

Priority	Question
People and safeguarding	Is anyone at immediate risk of harm, discrimination, exploitation, identity fraud, distress, self-harm or physical danger?
Containment	Can access, further disclosure, alteration or loss be stopped safely?
Evidence	What must be preserved to establish facts and support legal, disciplinary, insurance or criminal processes?
Continuity	Is access to safeguarding, medical, attendance or operational information disrupted?
Legal clock	When did Hindle's have a reasonable degree of certainty that a personal-data breach occurred?
Communication	Who needs accurate, controlled information and who must not be contacted yet?

9. Phase 1 - triage and containment

6. Open an incident record and note the date/time of awareness, reporter and lead.
7. Protect people first and initiate safeguarding or emergency action where required.
8. Recall or request deletion of misdirected information where safe, but do not rely on deletion confirmation alone.
9. Disable compromised accounts, revoke links/tokens, isolate devices or networks and preserve logs. Do not wipe, reimage or power off systems unless technical advice identifies this as necessary.
10. Recover physical records or devices where lawful and safe; report theft to police where appropriate.
11. Change affected credentials, enforce multi-factor authentication and review active sessions.
12. Secure backups and confirm that containment has not caused additional data loss.
13. Instruct relevant staff on confidentiality, evidence preservation and alternative working arrangements.

10. Misdirected email or disclosure

- Use recall where available and contact the unintended recipient through an appropriate channel, asking them not to read, copy, forward or use the information and to delete it securely.
- Request written confirmation, but assess risk on the assumption that access may have occurred.
- Do not send further sensitive information to explain the error.
- Record recipient identity, relationship, trustworthiness, response, data sensitivity, encryption and evidence of access.
- Consider whether contacting the recipient or affected person could increase safeguarding or legal risk.

11. Lost or stolen device or records

- Establish encryption, screen lock, remote-management capability, account access, contents, location and time missing.
- Attempt remote lock or wipe only through authorised support and preserve available audit evidence.
- Revoke sessions and credentials accessible from the device.
- Notify police, venue, transport operator or insurer where appropriate and retain the reference.
- Treat paper records and unencrypted devices as accessible unless evidence supports a different conclusion.

12. Cyber incident, phishing and ransomware

- Disconnect or isolate affected equipment as directed; do not continue using a suspected account.
- Do not pay a ransom, communicate with an attacker or run unapproved recovery tools.
- Preserve suspicious emails, headers, logs, messages and ransom notes.
- Engage authorised technical/cyber and insurance support and consider police or National Cyber Security Centre reporting.
- Assess both unauthorised access/exfiltration and loss of availability; restoration from backup does not remove confidentiality risk.
- Reset credentials from a known-safe device and increase monitoring after recovery.

13. Phase 2 - fact-finding

The investigation will be proportionate, time-bound and directed by the incident lead. Facts may develop after an initial notification, so the record will distinguish confirmed, likely and unknown information.

Area	Information to establish
Incident	What happened, cause, timeline, discovery, duration, containment and whether it is ongoing.
Data	Categories, sensitivity, format, volume, age, accuracy, encryption/pseudonymisation and ease of identification.
People	Approximate number, whether children or vulnerable people, and any particular personal circumstances increasing risk.
Access	Known or likely recipients, motive, capability, trustworthiness, evidence of viewing/copying and onward disclosure.
Consequences	Possible physical, financial, emotional, reputational, educational, employment, safeguarding or confidentiality harm.
Controls	Backups, encryption, access logs, deletion confirmation, recovery, monitoring and available protective action.
Responsibility	Whether Hindle's is controller, joint controller or processor and what contracts/commissioning arrangements require.

14. Phase 3 - risk assessment

Risk will be assessed from the perspective of affected individuals, not only Hindle's. The incident lead will consider likelihood and severity together and document the reasoning. Children, SEND, health, safeguarding, criminal-offence, financial and identity data normally require heightened scrutiny.

Indicative level	Characteristics and response
------------------	------------------------------

Low	Harm is unlikely because data is non-sensitive, exposure is very limited and effective controls make misuse improbable. Record and remediate; ICO notification normally not required.
Risk likely	There is a realistic possibility of adverse effects to rights and freedoms. Notify the ICO unless a legal exception applies; consider individual notification and protective support.
High risk	Serious harm is likely or plausible, particularly involving vulnerable people, safeguarding, identity/financial fraud, discrimination, blackmail, significant distress or danger. Notify affected individuals without undue delay unless an exception applies, as well as the ICO.

- Nature, sensitivity and volume of data.
- Ease of identification and strength of encryption or other controls.
- Number, age and vulnerability of people affected.
- Potential harm, including cumulative harm from combining data.
- Recipient or attacker capability, intent and opportunity.
- Duration and extent of exposure and evidence of access.
- Effectiveness of containment and steps individuals can take.

15. Awareness and the 72-hour period

For regulatory timing, Hindle's is aware when it has a reasonable degree of certainty that a security incident has compromised personal data. Staff must report immediately because internal investigation time is included in the 72-hour period. The incident record will state the awareness time and reasons. Uncertainty must not be used to delay initial assessment or a staged notification.

16. Phase 4 - notifying the ICO

Hindle's will notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours after awareness when the breach is likely to result in a risk to individuals' rights and freedoms. Notification is not required where such risk is unlikely, but that decision and evidence must be recorded.

- Nature of the breach, including categories and approximate numbers of people and records.
- Name and contact details of the data-protection lead or contact point.
- Likely consequences of the breach.
- Measures taken or proposed to address and mitigate it.
- Reasons for delay if notification occurs after 72 hours.

Where complete information is unavailable, Hindle's may provide an initial notification and further information in phases without undue delay. The Director will retain the ICO reference, submission and follow-up correspondence.

The 72-hour rule

The 72-hour period is not permission to wait three days. Internal notification must be immediate. External ICO notification is required only where the legal risk threshold is met.

17. Phase 5 - notifying affected individuals

Where a breach is likely to result in a high risk, Hindle's will communicate with affected individuals without undue delay unless a lawful exception applies. Communication will be clear, accessible and age appropriate and may involve parents/carers where appropriate to the child's competence, welfare and safeguarding circumstances.

- Describe the nature of the breach in plain language without exposing other people's information or compromising an investigation.
- Give the contact details of Joanne C. Hindle or another authorised contact point.
- Explain likely consequences and what Hindle's has done or will do.
- Give specific practical steps, such as changing passwords, monitoring accounts, avoiding scams, contacting a bank or seeking support.
- State how updates and complaints will be handled and the right to contact the ICO.

Direct communication may not be required where effective technical measures rendered the data unintelligible, later measures removed the high risk, or direct contact would involve disproportionate effort and an equally effective public communication is used. Any exception will be documented carefully.

18. Children, safeguarding and sensitive communications

- The DSL will assess whether notification could expose a child's location, family circumstances, protected address, allegations, health information or confidential safeguarding plan.
- Safety planning and statutory safeguarding information sharing must not be delayed by data-protection concerns.
- Where contacting a parent/carers could increase risk, the DSL will seek advice and identify a safe communication route.
- Affected learners will receive understandable reassurance and support without minimising the incident.
- Notifications must avoid blaming the child, reporter or accidental recipient.

19. Other notifications and coordination

- Commissioning school or local authority where the agreement, joint responsibilities or safeguarding require it.
- Relevant processor/controller and contractual contact.
- Insurer and approved cyber/legal advisers within policy conditions.
- Police where theft, fraud, harassment, hacking, extortion or other crime is suspected.
- National Cyber Security Centre or sector bodies where useful and appropriate.
- Ofsted, examination bodies or other regulators only where a specific duty or material regulatory concern applies.

20. Communications control

Only the Director or an authorised nominee may approve external breach communications. Staff must not comment to media, post online or communicate speculation. Messages will be accurate, consistent, compassionate and updated when material facts change. A communications log and copies of approved wording will be retained.

21. Phase 6 - recovery and remediation

- Restore from known-clean backups and validate accuracy, availability and security before normal operation.
- Apply security updates, remove malicious access, rotate credentials and review permissions.
- Correct or restore altered records and notify recipients where inaccurate information was shared.
- Provide practical support to affected people proportionate to risk.
- Replace insecure processes, devices or suppliers and update contracts where required.
- Increase monitoring for recurrence and preserve evidence for claims, investigation or enforcement.
- Complete safeguarding, disciplinary, complaint, insurer and commissioner actions as appropriate.

22. Lessons learned and closure

A breach is closed only when containment, risk decisions, required notifications, recovery and assigned corrective actions are documented. The Director will conduct a proportionate review covering root cause, human and system factors, response effectiveness, delays, communications, recurrence and policy/training needs. Serious or repeated breaches will receive a formal action plan with owners and deadlines.

23. Documentation and retention

Hindle's will document every personal-data breach, including facts, effects, risk assessment, decisions, notifications and remedial action, whether or not it is reported to the ICO. Records will be retained in accordance with the Records Retention Schedule, legal limitation periods, insurance, safeguarding and regulatory needs, with restricted access and secure disposal.

24. Prevention and preparedness

- Approved organisational accounts and systems only; no personal email, cloud storage, informal messaging, unapproved apps, removable media or AI tools for organisational data without written approval.
- Strong unique passwords, multi-factor authentication, supported software, updates, malware protection, screen locking and encryption where appropriate.
- Least-privilege access, individual accounts, periodic reviews and prompt removal when roles end or change.
- Encrypted secure transfer, careful recipient checks, BCC for appropriate group communication and minimised attachments.
- Secure paper storage, clear-desk/clear-screen practice, immediate collection of printing and confidential disposal.
- Tested backups and documented business-continuity and recovery arrangements.
- Processor due diligence, Article 28 terms and clear rapid-notification obligations.
- Induction, refresher training, phishing awareness and practical breach-response exercises.

25. Training, compliance and review

All staff and volunteers with access to personal data will receive breach-response training and must acknowledge this policy. Failure to report, deliberate misuse or concealment may result in disciplinary, contractual, safeguarding, regulatory or criminal action. This policy will be reviewed by 1 September 2027 or earlier following a significant incident, legal or regulatory change, new system or service, audit finding or change in risk.

Appendix A - Immediate Breach Report

Field	Record
Reporter / role / secure contact	
Date and exact time discovered	
Date and time reported to incident lead	
What happened and how discovered	
Systems, devices, records and locations affected	
Is it ongoing? Immediate danger or safeguarding risk?	
Data involved and approximate volume	
People affected, including children/vulnerability	
Known or possible recipients / attackers	
Containment already attempted	
Evidence preserved and location	
Support or urgent decision required	
Reporter signature / date	Received by / date and time

Appendix B - Data Breach Assessment and Notification Log

Assessment field	Decision and evidence
Breach reference / incident lead	
Awareness date/time and rationale	
Controller / processor / joint-controller status	
Confirmed timeline and cause	
Data categories, sensitivity, volume and security	
People affected: number, age and vulnerability	
Likely consequences and severity	
Likelihood, mitigating factors and residual risk	
Overall risk: low / risk likely / high risk	
ICO notification required? Reason	
ICO deadline / sent / reference / follow-up	
Individual notification required? Exception?	
Other organisations notified	
Recovery and corrective actions	
Closure approval / date	

Appendix C - 72-Hour Response Checklist

Timing	Required action
Immediately	Protect people; report to Joanne C. Hindle; open log; preserve evidence; contain safely; identify awareness time.
First hours	Engage DSL/technical/insurance support; identify systems, data and people; secure accounts and continuity; begin risk assessment.
Within 24 hours	Confirm key facts; assess likelihood/severity; draft ICO/individual communication if thresholds may be met; record unknowns.
Before 72 hours	Director decides ICO notification. Submit if risk is likely, even if phased information is necessary. Record reasons if not reporting.
Without undue delay	Notify individuals if high risk is likely; provide clear protective action and safe routes for children/vulnerable people.
After containment	Recover safely; monitor; investigate root cause; complete contractual/regulatory actions and corrective plan.
Closure	Confirm actions, notification records, lessons learned, owners/deadlines and policy/training updates.

Appendix D - Notification Content Checklist

ICO notification

Nature of breach; categories and approximate numbers of people/records; contact point; likely consequences; measures taken/proposed; reasons for any delay.

Individual notification

Plain-language breach description; contact point; likely consequences; action Hindle's has taken; practical protective steps; support, updates and complaint routes.