Data Breach Policy

Park Road Academy Primary School

Revised November 2026 for governing board approval

This policy explains how we recognise, report, contain, assess and learn from personal data breaches. It applies to staff, trustees and governors, volunteers, agency staff and others handling school information, including nursery and wraparound provision.

Policy control

Policy owner and operational lead: Mrs S Breen, Senior Responsible Individual
Contact: SRI@parkroadacademy.co.uk | 0161 972 4820
Accountable body: Governing Board
Previous policy: 2024–2026, ratified April 2024
Revised draft: 4 November 2026
Approval date: November 2026
Next review: Within one year of approval, or sooner following a significant incident or legal change

Immediate action for everyone

- Report any actual or suspected breach immediately to Mrs S Breen. Do not wait until the next working day or until a form is complete.
- If Mrs S Breen is unavailable, contact the Headteacher immediately; if unavailable, contact the Deputy Headteacher or senior leader on duty using the school's internal emergency contact arrangements.
- Take safe, proportionate steps within your authority to stop further disclosure and preserve evidence. Obtain urgent IT or safeguarding support where needed.
- The ICO deadline runs in calendar hours, including nights, weekends and school holidays.

Before adoption, the Headteacher must confirm and circulate the named deputy and the internal out-of-hours contact route. Personal emergency contact details must be kept in a restricted operational contact list, not in the published policy.

1 Scope and definitions

We follow the UK GDPR and the Data Protection Act 2018, as amended. Read this policy alongside the school's Data Protection Policy, safeguarding procedures, acceptable use and cyber security arrangements, records retention schedule and business continuity arrangements.

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It can affect confidentiality, integrity or availability, in any format, including paper, verbal information and electronic records. Temporary loss of access can also be a breach.

Personal data is information relating to an identified or identifiable living person. Pseudonymised information remains personal data where it can be linked back to someone. Special category data includes health, ethnicity, religion, trade union membership, sex life or sexual orientation, genetic data and biometric data used for unique identification. Criminal offence data is separately protected and is not special category data.

- Examples include an email or attachment sent to the wrong person, exposed addresses or safeguarding records, misplaced files, insecure disposal, lost devices, unauthorised access, phishing and ransomware.
- Report suspected incidents and near misses even if no harm is apparent. A general IT incident may need action even if it is not a personal data breach.
- All personal data breaches must be recorded. Not every breach needs to be reported to the ICO or to affected individuals.

2 Responsibilities and escalation

The Governing Board retains oversight of the school's compliance. The Headteacher ensures that incidents receive prompt resources and leadership, that cover is available and that required notifications are made on behalf of the school as controller.

Mrs S Breen, Senior Responsible Individual (SRI), coordinates incident logging, containment, investigation and follow-up, and provides data protection advice. Decisions and advice must be recorded. The Headteacher must seek independent specialist advice where a conflict arises, including where the incident concerns the SRI's own actions.

All personnel must report promptly, cooperate with authorised investigations and follow instructions. IT support provides technical containment, recovery and evidence preservation. The DSL must be involved immediately where information exposure or loss may create a safeguarding risk. Do not delay safeguarding action while completing the data breach process.

Processors must notify the school without undue delay after becoming aware of a personal data breach, assist with investigation and provide updates. These obligations, including subcontractor reporting and suitable contact arrangements, must be reflected in processing contracts.

3 Containment and recovery

The incident lead must act immediately, record decisions and coordinate appropriate assistance. Staff must not investigate beyond their authority, contact an attacker, or notify regulators or affected individuals independently. This does not prevent safe urgent containment or safeguarding action.

- Establish what happened, when it occurred, when it was discovered and when the school became aware that personal data had been compromised. Record who knows and what remains uncertain.
- Stop further disclosure: restrict access or sharing, recall an email where possible, and ask unintended recipients not to use or forward the information and to confirm secure deletion. Recall alone is not proof of containment.
- Contact IT urgently for suspected account compromise, lost devices or malware. IT may isolate devices, revoke access, reset credentials, secure logs and consider remote locking or wiping. Preserve evidence before destructive actions where practicable.
- Locate paper records, secure remaining information and restore access from verified clean backups when appropriate. Assess the effect of lost availability on safeguarding, medical support and school operations.
- Keep an incident chronology and protect logs, messages and other evidence. Do not circulate breached information unnecessarily or copy it into insecure reporting channels.
- Consider police or other relevant reporting, insurers and specialist cyber support. Check insurance notification conditions promptly without delaying legal notifications.

4 Assessment of risk to people

The incident lead, with SRI advice, must assess both the likelihood and severity of harm to individuals, using the facts available. Reassess as information emerges; do not wait for the full investigation before making notification decisions.

- Identify the categories of people, approximate numbers of people and records, the data involved, its sensitivity and how easily people can be identified.
- Consider who received or accessed it, whether it has been copied or published, exposure duration, recovery and deletion evidence, and whether encryption was effective with keys kept secure. Password protection alone does not establish that information is safe.
- Consider distress, discrimination, identity fraud, financial loss, confidentiality loss, reputational harm and physical danger. Give particular attention to children, vulnerable people, medical information, safeguarding records, court restrictions and protected addresses.
- Assess harm caused by inaccurate or unavailable information, even where no information appears to have been stolen.
- Record the reasoning, mitigating measures, uncertainty and next review time. Risk to the school's reputation does not replace assessment of risk to people.

5 Notification decisions

5.1 Notification to the ICO

Notify the ICO unless the personal data breach is unlikely to result in a risk to individuals' rights and freedoms. A high risk is not required for ICO notification. The school must notify without undue delay and, where feasible, within 72 hours of becoming aware of the breach. This is not 72 working hours and does not start when the SRI completes an investigation.

The SRI coordinates the submission with the Headteacher. If the usual lead is absent, the Headteacher or delegated senior leader must act. Seek urgent advice where the threshold is uncertain, without allowing uncertainty to cause avoidable delay.

Provide the nature of the breach; categories and approximate numbers of people and records affected where possible; SRI or other contact details; likely consequences; and measures taken or proposed, including mitigation. Submit available information first and provide updates in phases without undue further delay. If notification is late, give the ICO reasons and retain them in the incident record.

Record the decision and supporting risk assessment whether or not a report is made, including the decision maker, time, notification reference and any later reassessment.

5.2 Informing affected individuals

Where a breach is likely to result in a high risk to individuals' rights and freedoms, inform those affected directly and without undue delay, in clear and plain language. Do not wait for an ICO response. For children, decide how to communicate appropriately with the child and/or parent or carer, considering understanding, parental responsibility, safeguarding and any restrictions on contact.

Explain what happened, provide SRI or other contact details, describe likely consequences and the steps taken or proposed, and give practical protective advice and support. Use an accessible communication method appropriate to the recipient. Appendix 3 is a blank adaptable template.

Direct notification is not required where effective measures rendered the affected data unintelligible to unauthorised people; subsequent measures ensure the high risk is no longer likely to materialise; or direct notification would involve disproportionate effort. In the last case, a public communication or similarly effective measure is required. Record the evidence and SRI advice supporting any exception. The ICO can require notification.

The school may also choose to inform people below the high-risk threshold where this helps them protect themselves or supports transparency. Record the reason and consider safeguarding before communicating.

5.3 Other parties

Consider notifications to the DSL and safeguarding partners, IT provider, insurers, police, relevant authorities, other controllers and affected suppliers as appropriate. Share only necessary information securely. Coordinate public statements through the Headteacher and protect confidentiality.

6 Investigation and improvement

The SRI must establish the sequence of events and root causes, checking what safeguards existed, whether they were followed, whether training was adequate and whether earlier concerns or incidents identified the risk. Consider human error, process design and technical weaknesses together.

Agree an action plan with named owners and completion dates. Actions may include improved access controls, document naming and storage, checking recipients and attachments, secure disposal, revised supplier arrangements, backup testing, updated procedures and targeted training. Review the ROPA, DPIAs, privacy notices and security assessments where the incident reveals a relevant change or gap.

The SRI monitors actions to completion, checks their effectiveness and records closure. Reopen the assessment if new evidence changes risk. Provide proportionate reports to the Headteacher and governing board, using anonymised or minimised information wherever possible, and review recurring incidents and near misses.

Prompt reporting of mistakes is encouraged. Any concerns about deliberate misuse, concealment or reckless conduct must be considered fairly under relevant HR procedures, taking appropriate advice. Reporting an honest error does not itself determine disciplinary action.

7 Records and retention

Maintain a secure breach register and linked incident files covering all confirmed personal data breaches, including those not notified externally. Record suspected incidents and near misses sufficiently to support learning, identifying their final classification.

Records must include the facts, effects, assessment, containment, advice, decisions and reasons, communications, action owners, deadlines and closure evidence. Restrict access to those who need it. Store actual incident records separately from the policy and blank forms.

Retain incident records under the school's approved retention schedule, taking account of legal advice, claims, safeguarding and any investigation or preservation hold. Review and securely dispose of records when retention is no longer justified. Do not delete evidence subject to an active hold.

8 Training and review

Provide training at induction, regular refreshers, and additional guidance when procedures, threats or legislation change and following relevant incidents. Staff must know the reporting and cover arrangements. Record attendance and acknowledgement of revised procedures.

Review this policy at least annually and following significant incidents or relevant legal changes. The Headteacher must keep the restricted emergency contact list current and ensure cover works during absences, weekends and holidays.

Appendix 1 Incident reporting form

Restricted when completed. Report immediately before completing this form. Use an incident reference and keep unnecessary personal details out of the report. Attach additional secure pages as needed.

Incident reference and reporter name or role

_____

Date and time of incident or estimated period

_____

Date and time discovered and by whom

_____

Date and time school became aware of a personal data breach

_____

Reported to whom and when including escalation or delay

_____

What happened and systems locations or suppliers involved

_____

People and data affected including approximate numbers and sensitive information

_____

Immediate containment recovery and evidence preserved

_____

Potential harm including safeguarding concerns and DSL involvement

_____

Appendix 1 Assessment and closure record

To be completed by the incident lead with SRI advice. Link supporting evidence securely.

Risk assessment including likelihood severity safeguards and remaining uncertainty

_____

ICO decision and reasons including decision maker date time and 72 hour deadline

_____

ICO submission time reference updates and reasons for any delay

_____

Decision on informing individuals including high risk test or exception and reasons

_____

Other notifications and advice including safeguarding IT insurers or police

_____

Root causes and whether existing controls and training were adequate

_____

Action plan including owner deadline and completion evidence

_____

Reassessment dates final outcome closure date and approving lead

_____

Appendix 2 Risk assessment prompts

Use these prompts to support a reasoned assessment, not to assign automatic notification outcomes. One person's information can create a high risk. A large incident is not automatically high risk if the data was effectively protected.

Unlikely risk to people

An example may be a limited disclosure to a trusted recipient who provides reliable confirmation of deletion before use, with no sensitive context. Record why harm is unlikely. All confirmed breaches remain in the register even where ICO notification is not required.

Risk requiring ICO notification

Examples may include exposure of usable identity or financial details, uncontrolled sharing of confidential records, or loss of access to essential personal data with harmful consequences. Notify unless risk is unlikely; consider separately whether risk is high enough to require direct notification.

High risk requiring direct notification

Examples may include exposure of a protected address, safeguarding allegations, exploitable identity details or highly sensitive records where serious harm is likely. Involve the DSL immediately where relevant and inform affected people without undue delay unless a documented statutory exception applies.

Questions to record

- What could happen to the people concerned and how serious would it be?
- How likely is that harm given the actual recipient, exposure and containment evidence?
- Are any children or other people especially vulnerable in this situation?
- What does encryption or deletion evidence actually establish?
- Would loss of availability or inaccurate data interfere with care, safety or access to support?
- What can the school and affected individuals do now to reduce harm?
- When must the assessment be reviewed and who owns that review?

General IT conduct issues without a personal data breach should be managed under the relevant security or HR process. They must still be escalated if they suggest a wider information risk.

Appendix 3 Notification to affected individuals

Template for adaptation and approval by the incident lead with SRI advice. Replace every bracketed field. Check recipient details and safeguarding restrictions. Do not include information about other people unnecessarily.

Dear [name],

We are writing to inform you about a personal data breach affecting [your information / information about your child]. We are sorry this has happened.

What happened

[Explain the nature of the incident, relevant dates and how it was discovered in clear language. Distinguish confirmed facts from matters still being investigated.]

Information affected

[Describe the categories of personal information affected and the relevant person or people. Explain what is known about who could access it.]

What this may mean for you

[Describe the likely consequences and any uncertainty. Give an individual assessment where appropriate without minimising potential harm.]

What we have done

[Explain containment, recovery, protective measures, ongoing investigation and steps to prevent recurrence. Include ICO notification status where appropriate.]

What you can do and support available

[Give specific, proportionate protective advice and explain the support the school can provide. Say when further updates will be available, where possible.]

Contact us

If you have questions or need support, please contact Mrs S Breen, Senior Responsible Individual, at SRI@parkroadacademy.co.uk or on 0161 972 4820. You can also raise a data protection concern with the Information Commissioner's Office at https://ico.org.uk/make-a-complaint/.

Yours sincerely
[Name and role]
For Park Road Academy Primary School

Reference guidance

ICO: Personal data breaches a guide
https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/
DfE: Data protection in schools Managing breaches of data
https://www.gov.uk/guidance/data-protection-in-schools/managing-breaches-of-data
Guidance checked for this revision: 4 November 2026.