Carleton Green Community Primary School

Fly high. Soar

Data Breach Policy

2026-2027

Approved by: Stacey Clark	**Date:** July 2026
Last reviewed on: July 2025	
Next review due by: July 2027	

DATA BREACH POLICY

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed, or supplied. It requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure, or destruction of personal data.

The UK GDPR places obligations on staff to report actual or suspected data breaches, and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with its provisions. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the School of any data breach without undue delay after becoming aware of it. Failure to do so may result in a breach of the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal, depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the school and is not intended to have contractual effect. Changes to data protection legislation will be monitored, and further amendments may be required in order to remain compliant with legal obligations.

Definitions

- **Personal Data:** Any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data, but excludes anonymous data or data where the identity of an individual has been permanently removed. Personal data can be factual (e.g., name, email address, location, date of birth) or an opinion about that person's actions or behaviour. Personal data will be stored either electronically or as part of a structured manual filing system so that it can be retrieved automatically by reference to the individual or criteria relating to them.

- **Special Category Data:** Previously termed "Sensitive Personal Data", Special Category Data refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data, and personal data relating to criminal offences and convictions.

- **Personal Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored, or otherwise processed.

- **Data Subject:** The person to whom the personal data relates.

- **ICO:** The Information Commissioner's Office, the UK's independent regulator for data protection and information.

Responsibility

- The Headteacher has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.
- In the absence of the Headteacher, please contact the School Business Manager.
- The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines. Please contact the DPO with any questions about the operation of this policy or UK GDPR, or if you have concerns that this policy is not being followed.

The DPO's contact details are set out below: -

Contact details for the council's data controller are:
Information Governance Team
Lancashire County Council
PO Box 78
County Hall
Preston
PR1 8XJ

Email: dataprotection@lancashire.gov.uk

Security and Data-Related Policies

Staff should refer to the following related policies, available from the office:

- **Security Policy**: Guidelines and processes on keeping personal data secure against loss and misuse.
- **Data Protection Policy:** Obligations under UK GDPR on how personal data is processed.
- **Cyber Security Policy:** Obligations and guidelines for cyber security issues.
- **Acceptable Use Policy (AUP):** Guidance regarding the safe use of communication channels, devices, and messaging platforms.

Data Breach Procedure

What Is A Personal Data Breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored, or otherwise processed.

Examples include, but are not limited to:

- Loss or theft of data or equipment on which data is stored (e.g., loss of a laptop, USB stick, or paper file).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (e.g., sending an email, document, or SMS to the wrong recipient).
- Unauthorised Third-Party Messaging: Using non-approved personal communication apps (e.g., WhatsApp) or personal devices to communicate pupil data, safeguard details, or staff information between colleagues or external parties.
- Unforeseen circumstances such as a fire or flood.
- Hacking, phishing, and other "blagging" attacks where information is obtained by deceiving whoever holds it.

Important Directives for Staff: Messaging & Instant Apps

- **Prohibition of WhatsApp & Personal Messaging Platforms:** Staff are strictly prohibited from using WhatsApp, personal SMS, or any other unapproved messaging platforms on personal mobile phones/devices to share, discuss, or send school-related data, pupil details, safeguarding concerns, or personnel information to other teachers or third parties.
- **Approved Channels Only:** All work-related correspondence containing personal or sensitive information must strictly occur via official school channels (e.g., official school email, designated secure management information systems [MIS], or approved learning platforms).
- **Risk of Non-Compliance:** Unencrypted or unmonitored personal messaging apps create significant security vulnerabilities and expose the school to regulatory fines and data protection breaches. Transgressions will be managed under the school's Disciplinary Policy.

When Does It Need to Be Reported?

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means the breach needs to be more than just losing personal data—if unaddressed, the breach is likely to have a significant detrimental effect on individuals. Examples of a significant effect include:

- Potential or actual discrimination.
- Potential or actual financial loss.
- Risk to physical safety or reputation.
- Exposure to identity theft (e.g., release of non-public identifiers such as passport details).
- Exposure of private aspects of a person's life.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, those individuals must also be notified directly.

Reporting a Data Breach

If you know or suspect a personal data breach has occurred or may occur, you must:

1. Immediately complete a Data Breach Report Form / Email and submit it to your line manager.
2. Seek advice from your line manager or the DPO if you are unsure whether a breach should be reported. Breach reporting is actively encouraged across the school.
3. Do not take any further action once reported. In particular, do not notify affected individuals/regulators or investigate further on your own. The line manager will acknowledge receipt and handle the incident in collaboration with the DPO.

Managing and Recording the Breach

Upon notification, the line manager and DPO will take immediate steps to:

1. Contain the breach.
2. Recover, rectify, or delete the data lost, damaged, or disclosed where possible.
3. Assess and record the breach in the School's Data Breach Register.
4. Notify the ICO (where required).
5. Notify affected data subjects (where required).
6. Notify other appropriate authorities.
7. Take steps to prevent future breaches.

Notifying the ICO

The DPO or Headteacher will notify the ICO without undue delay and, where possible, within 72 hours of becoming aware of a risk-bearing breach. The 72-hour deadline applies continuously, including during school holidays. If in doubt, the default assumption is to report. Written reasons will be documented if a report exceeds 72 hours.

Notifying Data Subjects

When a breach poses a high risk to individual rights and freedoms, the Headteacher/DPO will inform affected individuals without undue delay. This includes providing DPO/ICO details, likely consequences, and remediation steps. If direct notification requires disproportionate effort, public notifications (e.g., a statement on the school website) may be evaluated.

Notifying Other Authorities

Where relevant, the school will consider notifying additional parties such as:

- Insurers
- Parents/Guardians
- Impacted third parties
- Local Authority
- Police (e.g., in cases of stolen hardware or criminal activity)

Assessing & Preventing Future Breaches

Following containment, the school will conduct an investigation to analyse security measures, vulnerability risks, data sensitivity, and overall impact.
To prevent future incidents, the school will:

- Evaluate existing technical and organizational controls.
- Address staff awareness gaps through targeted training or guidance.
- Perform privacy or Data Protection Impact Assessments (DPIAs) where necessary.
- Update the Data Breach Register and debrief the Governing Body.

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an afterthought. Staff are strongly encouraged to report any data security concerns or potential risks (even if they do not meet full breach threshold criteria) to the Headteacher or DPO immediately.

Training & Monitoring

The school will ensure all staff receive training to detect and report data breaches effectively. This policy will be distributed to all staff. The effectiveness of these procedures will be regularly monitored and formally reviewed to ensure ongoing operational compliance and risk reduction.