Bushfield Road Infant School

Data Protection and Records Management Policy

Data Protection Officer (DPO): North Lincolnshire Council
Approved by: Governing Body
Date approved: November 2026
Review date: November 2027

1. Purpose and scope

Bushfield Road Infant School respects the privacy of pupils, families, staff, governors, volunteers, visitors and other people whose personal information it uses.

This policy explains how the school collects, uses, stores, shares, retains and securely disposes of personal information. It applies to all staff, governors, volunteers, contractors and other people working on the school's behalf, and to information held in paper, electronic, photographic, audio or video form.

Everyone covered by this policy must handle personal information lawfully, fairly, securely and only when needed for their role.

2. Legal framework

The school will handle personal information in accordance with applicable data protection law, including the UK General Data Protection Regulation, the Data Protection Act 2018 and the Data (Use and Access) Act 2025.

The school will also have regard to relevant education, safeguarding, freedom of information and records-management requirements.

3. Roles and responsibilities

The governing body is accountable for the school's compliance with data protection law. It will oversee the school's arrangements and receive assurance about compliance and risks.

The Headteacher is responsible for ensuring that suitable day-to-day procedures are in place, staff understand their responsibilities, and suspected data breaches are escalated promptly.

The DPO advises the school, monitors compliance, supports information-rights requests, advises on data protection risks and impact assessments, and acts as a contact point for individuals and the Information Commissioner's Office (ICO). The DPO must be able to perform this role impartially.

All staff and other authorised users must:

- access personal information only when needed for their role;
- follow this policy and the school's security procedures;
- keep information accurate and report errors;
- share information only through approved, secure channels;
- report a suspected loss, disclosure or other data breach immediately to the Headteacher and DPO; and
- complete required data protection training.

The school is the data controller for the personal information it determines how and why to use. Where another organisation processes information on the school's behalf, the school will use appropriate contractual arrangements and check that the provider offers suitable safeguards.

4. How the school uses personal information

The school uses personal information to carry out its education and safeguarding responsibilities and to manage its services. This may include information about:

- pupils and their parents or carers;
- staff, governors, volunteers and job applicants;
- attendance, learning, progress and educational support;
- health, special educational needs and safeguarding;
- finance, employment and school administration; and
- visitors, suppliers and contractors.

The school will identify and document a lawful basis for each purpose. Depending on the purpose, this may include legal obligation, public task, contract, legitimate interests, vital interests or consent. Special-category information, such as health or ethnicity, and criminal-offence information require additional legal conditions and safeguards.

Consent is not the school's default legal basis. Where consent is used, it must be freely given, specific, informed and recorded. The school will explain how consent can

be withdrawn. Withdrawing consent does not affect processing already carried out lawfully, and it does not require the school to delete information where another lawful basis or legal retention requirement applies.

5. Fairness, accuracy and minimisation

The school will:

- tell individuals what information it collects, why it uses it, who it may share it with and how long it keeps it, through clear privacy notices;
- collect information that is relevant and necessary for the stated purpose;
- take reasonable steps to keep information accurate and up to date;
- correct inaccurate information where appropriate;
- limit access to people who need the information for their work; and
- review whether information is still needed and dispose of it securely when its retention period ends.

Privacy notices will be reviewed when the school's processing changes and at least annually.

6. Sharing information

The school may share personal information where there is a lawful basis to do so—for example, to meet legal duties, support a pupil's education or welfare, protect a child, or provide a contracted service.

Information may be shared with organisations such as the local authority, another school, health services, social care, the police, the Department for Education or an approved service provider, where appropriate and lawful.

Staff must not assume that consent is always required before sharing safeguarding information. Case-specific safeguarding concerns must be managed by the school's Designated Safeguarding Lead (DSL) through the school's established safeguarding procedures. Staff must not delay an appropriate safeguarding referral while seeking data protection advice.

Before sharing information, staff must check that:

- the sharing is necessary and lawful;
- only information relevant to the purpose is shared;
- the recipient is authorised to receive it; and
- an approved secure method is used.

Where appropriate, the school will have a data-sharing agreement or data-processing contract in place.

7. Security and confidentiality

The school will use proportionate technical and organisational safeguards to protect personal information from unauthorised access, loss, alteration or disclosure.

Staff must:

- use individual accounts and strong passwords, and never share login details;
- lock screens and secure paper records when not in use;
- check recipients carefully before sending emails or attachments;
- use approved school systems and secure methods to access or transfer information;
- avoid storing school information on personal devices or personal accounts unless specifically authorised and appropriately secured;
- keep confidential information out of sight of visitors and people who do not need access; and
- dispose of confidential paper and electronic information using approved secure methods through North Lincolnshire Council.

The school will maintain appropriate access controls, backups and arrangements for responding to cyber incidents.

8. Personal data breaches

A personal data breach may include information being sent to the wrong person, a device or file being lost, information being accessed without authority, or data being altered, destroyed or made unavailable.

Anyone who becomes aware of a suspected breach must report it **immediately** to the Headteacher and DPO. Staff must not investigate or notify affected individuals or the ICO on their own initiative unless authorised to do so.

The Headteacher and DPO will:

1. take prompt steps to contain the incident and protect individuals;
2. establish what happened, what information and people are affected, and the likely consequences;
3. record the incident and the decisions made, including the reasons for reporting or not reporting;
4. decide whether the breach must be reported to the ICO; and
5. notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

Where a breach is reportable, the school must notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. **The 72-hour period is not a general deadline for notifying affected individuals.** Those individuals must be told without undue delay when the high-risk threshold applies.

9. Individual rights and requests

People have rights over their personal information, which may include the right to access it, correct it, request erasure or restriction, object to processing, or request data portability. These rights are subject to legal conditions and exemptions; a request to erase information does not automatically mean the school must delete it.

Requests can be made verbally or in writing. Any member of staff who receives a request must pass it promptly to the Headteacher and DPO. Staff must not make a decision about whether to grant or refuse a request.

The school will:

- establish the requester's identity or authority where reasonably necessary;
- clarify a request where needed and handle any pause in the response period in line with current requirements;
- carry out a reasonable and proportionate search;
- protect other people's information when responding; and
- respond without undue delay and normally within one calendar month, subject to applicable rules on clarification, complexity, extensions and exemptions.

The school will explain the outcome and any available route to complain to the ICO where required.

10. Children's information

The school recognises that children have their own data protection rights. A parent or carer does not automatically have a right to access all information about a child. Requests relating to a pupil will be considered in light of the child's age, understanding, rights, welfare and the circumstances of the request.

Where a request raises a safeguarding or welfare concern, the school will involve the DSL and DPO as appropriate. Information will only be disclosed where lawful and in the child's best interests.

11. Records, retention and disposal

The school will maintain a records-retention schedule that identifies what records are held, why they are needed, how long they will be kept and how they will be disposed of.

Records will not be kept for longer than necessary, except where a legal requirement, ongoing matter or other documented reason requires longer retention. The school will review its retention schedule at least annually and securely destroy or delete information when the applicable period ends.

Pupil records will be managed and transferred in accordance with current education and records-management guidance. The school will not apply a blanket retention period to all pupil records; different records have different requirements. The existing policy's statement that a primary pupil record is generally kept until the pupil reaches 25 should therefore be removed and replaced by the school's approved retention schedule.

The school will keep an appropriate record of authorised destruction.

12. Data protection by design

When introducing a new system, service or use of personal information, the school will consider privacy and security from the outset. The DPO will advise whether a data protection impact assessment is needed, particularly where processing could create a high risk to individuals.

13. Training, monitoring and review

Staff and governors will receive appropriate data protection information at induction and periodic refresher training. The DPO will support the school to monitor compliance, review procedures and advise the governing body on significant risks.

This policy will be reviewed annually and sooner if there are relevant changes to legislation, guidance, the school's systems or the way personal information is used.