Newburn Manor Nursery School



Monkchester Road Nursery



Ashfield Nursery School

Newcastle Nursery Schools' Federation

Data Protection and Confidentiality Policy

October 2026
To be reviewed October 2027

Newcastle Nursery Schools' Federation is committed to protecting the privacy, confidentiality, integrity and security of personal information relating to children, families, staff, governors, volunteers, contractors and visitors.

The school recognises its responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Human Rights Act 1998, Freedom of Information legislation, and safeguarding requirements. We will ensure that all personal information is processed lawfully, fairly, transparently and securely.

The school acknowledges that confidentiality is essential in maintaining trust with children, families, staff and partner agencies whilst recognising that safeguarding concerns may require information sharing where a child is at risk of harm.

This policy aims to:

- Ensure compliance with data protection legislation.
- Protect the rights and privacy of individuals.
- Ensure personal information is held securely and only accessed when necessary.
- Promote a culture of confidentiality and professional responsibility.
- Provide clear guidance on information sharing.
- Support safeguarding and promote the welfare of children.

This policy applies to:

- All employees.
- Governors.
- Volunteers.
- Students on placement.
- Consultants and contractors.
- Agency staff.
- Any individual handling personal information on behalf of the school.

This policy covers all information held in:

- Paper records.
- Electronic systems.
- Emails.
- Photographs and video recordings.
- CCTV images (where applicable).

- Portable devices.
- Cloud-based storage systems.

The school will comply with the UK GDPR principles by ensuring personal data is:

Lawful, Fair and Transparent

- Personal information will only be collected and processed where there is a lawful basis and individuals are informed about how their information is used.

Collected for Specified Purposes

- Data will only be collected for legitimate educational, employment, safeguarding or administrative purposes.

Adequate, Relevant and Limited

- Only information necessary for the intended purpose will be collected and retained.

Accurate and Up to Date

- Reasonable steps will be taken to ensure information is accurate and amended when necessary.

Kept for No Longer Than Necessary

- Records will be retained in accordance with statutory requirements and the school's retention schedule.

Secure

- Appropriate technical and organisational measures will be used to protect personal data from loss, misuse, unauthorised access, disclosure or destruction.

Accountable

- The school will demonstrate compliance through policies, procedures, training and monitoring.

Definitions

Personal Data

Any information relating to an identified or identifiable individual.

Examples include:

- Names.
- Addresses.
- Dates of birth.
- Contact details.
- Assessment records.
- Employment records.
- Photographs.

Special Category Data

Information requiring additional protection, including:

- Health information.
- Ethnicity.
- Religious beliefs.
- Biometric data.
- Information concerning disabilities or special educational needs.

Roles and Responsibilities

Governing Body

The Governing Body is responsible for ensuring the school complies with data protection legislation and maintains effective governance arrangements.

Headteacher

The Headteacher is responsible for:

- Implementing this policy.
- Ensuring staff understand their responsibilities.
- Managing data breaches.
- Overseeing data protection practices.

Data Protection Officer (DPO)

The school's appointed Data Protection Officer will:

- Monitor compliance.
- Provide advice and guidance.
- Investigate data breaches.
- Act as a point of contact with the Information Commissioner's Office (ICO).

Staff

All staff must:

- Follow this policy.
- Protect confidential information.
- Report actual or suspected data breaches immediately.
- Undertake data protection training as required.

Confidentiality

General Principles

Information about children, families and staff must be treated as confidential.

Information will only be shared:

- With authorised individuals who need the information for their role.
- With parental consent where appropriate.
- Where there is a legal obligation.
- Where safeguarding concerns require disclosure.

Staff must not:

- Discuss confidential information in public areas.
- Disclose information to unauthorised persons.
- Access records without a legitimate reason.
- Remove confidential records from the premises without permission.

Confidentiality and Safeguarding

The welfare of the child is paramount.

Where staff have concerns about a child's safety or wellbeing, confidentiality cannot be guaranteed.

Information may be shared with:

- Children's Social Care.
- Police.
- Health professionals.
- Other relevant agencies.

Where possible, information sharing decisions will be recorded.

The school will follow safeguarding procedures as outlined in its Child Protection and Safeguarding Policy.

Collection and Use of Information

The school collects information in order to:

- Provide education and care.
- Safeguard children.
- Monitor progress and development.
- Support special educational needs.
- Meet statutory obligations.
- Manage employment and payroll functions.
- Communicate with parents and carers.

Privacy notices will explain:

- What information is collected.
- Why it is collected.
- How it will be used.
- Who it may be shared with.
- How long it will be retained.
- Individual rights.

Information Sharing

Information may be shared:

Internally

When necessary for:

- Education and learning.
- Safeguarding.
- Administration.
- Employment management.

Externally

With:

- Local Authorities.
- Department for Education.
- Social Care services.
- Health services.
- Professional advisers.
- Regulatory bodies.

Information sharing will be:

- Lawful.
- Proportionate.
- Relevant.
- Secure.

Security of Information

The school will implement measures including:

Physical Security

- Locked filing cabinets.
- Secure offices.
- Visitor controls.
- Appropriate disposal of records.

Electronic Security

- Password-protected systems.
- Encryption where appropriate.
- Secure networks.
- Access controls based on job role.
- Anti-virus and cyber security measures.

Remote Working

Staff accessing information remotely must:

- Use authorised devices.
- Keep records secure.
- Prevent unauthorised viewing.
- Follow school ICT security procedures.

Photographs, Videos and Images

Photographs and videos of children will only be used:

- In accordance with parental permissions.
- For educational purposes.
- To celebrate achievements.
- For publicity where consent has been obtained.

Images will be stored securely and only retained for as long as necessary.

CCTV

Where CCTV is installed, it will:

- Operate for safety and security purposes.
- Be managed in accordance with data protection requirements.
- Be accessed only by authorised personnel.

Appropriate signage will be displayed.

Retention and Disposal of Records

The school will:

- Maintain a records retention schedule.
- Retain records only as long as required.
- Dispose of information securely when no longer needed.

Secure disposal methods may include:

- Confidential shredding.
- Approved destruction services.
- Secure deletion of electronic records.

Data Subjects' Rights

Individuals have rights under UK GDPR including:

- Right to be informed.
- Right of access.
- Right to rectification.

- Right to erasure (where applicable).
- Right to restrict processing.
- Right to data portability.
- Right to object.
- Rights relating to automated decision-making.

Requests should be made in writing to the Headteacher or Data Protection Officer.

Subject Access Requests

The school will respond to Subject Access Requests in accordance with legal requirements.

The school may:

- Verify identity before releasing information.
- Request clarification where necessary.
- Withhold information where exemptions apply.

A record of requests and responses will be maintained.

Data Breaches

A personal data breach may include:

- Loss of records.
- Sending information to the wrong person.
- Unauthorised access.
- Cybersecurity incidents.

Staff must report breaches immediately to the Headteacher and/or Data Protection Officer.

The school will:

- Investigate all breaches.
- Assess risk.
- Take corrective action.
- Notify the ICO and affected individuals where required.

Training and Awareness

All staff will receive:

- Data protection induction training.
- Ongoing updates and refresher training.
- Information governance guidance relevant to their role.

Staff are expected to maintain high standards of confidentiality at all times.

Monitoring and Review

The Governing Body and Headteacher will monitor the implementation of this policy.

The policy will be reviewed:

- Annually; or
- Following legislative changes; or
- Following significant data protection incidents.

Linked Policies

- Child Protection and Safeguarding Policy
- Online Safety Policy
- ICT Acceptable Use Policy
- Staff Code of Conduct

Equality Impact Statement

Newcastle Nursery Schools' Federation will ensure that this policy is applied fairly, consistently and in accordance with the Equality Act 2010. No individual will be disadvantaged on the grounds of protected characteristics.