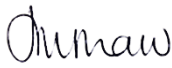




Data Protection Policy Statement 2026/27

Written by	Ms Eilidh Cook/JShaw
Date for review	September 2027
Signed by Headteacher	
Signed by SLT	 
Review Dates confirmed	April 2020 updated, February 2022

	September 2024 September 2025 September 2026
--	---

Data Protection Statement

New York Primary School is fully committed to full compliance with the requirements of the General Data Protection Regulation (GDPR) and The Data Protection Act 2018. The School will therefore follow procedures which aim to ensure that all our staff, Governors, and contractors who have access to any personal data held by or on behalf of the School are fully aware of and abide by their duties under the GDPR. We also adhere to the guidance issued by the [Information Commissioner](#).

Policy Statement

We collect and use information about our pupils in order to carry out our functions. This also includes information about current, past and prospective staff, pupils and parents and suppliers of services to us. In addition we are required by law to collect and use information in order to comply with statutory requirements. Personal information must be processed appropriately however it is collected, recorded and used and in whatever format it is held.

We regard the handling of personal information as very important to us being able to carry out our day to day business and essential to maintaining confidence. We therefore fully adhere to the Principles of the GDPR. We only process personal data when we have a legal basis to do so. For a primary school the legal bases are:

Public Task – a statutory duty e.g. tracking academic information, progress attendance

Legal Obligation – to comply with laws regarding safeguarding and statutory testing and DfE census reporting

Vital Interests – to protect someone in an emergency i.e. sharing medical details with relevant services

Consent – where no statutory duty applies e.g. school photographs and app use where consent is given and can be withdrawn. In school we obtain written consent from parents before publishing photographs or videos of pupils on the school website, social media or local press.

Specific to a primary school under KCSiE, safeguarding takes priority and school will share relevant safeguarding data with local authorities and agencies to protect the welfare of a child.

How we handle personal and sensitive data

We will ensure that appropriate controls and measures are in place to monitor and review data so:

- It is secure and protected
- It is used in efficient and effective ways to improve the education of our pupils
- Only necessary data is collected
- It is only collected for the purpose as described at the time of collection
- Information is accurate
- Information is not kept for longer than is necessary
- Data which is no longer needed is securely destroyed
- Information is not transferred abroad without suitable safeguards
- There is general information for pupils and parents and staff of their rights to access information
- The rights of pupils, parents and staff about whom information is held can be fully exercised under the General Data Protection Regulations.

We will also ensure appropriate technical and organisational security measures to safeguard information (including unauthorised or unlawful processing and accidental loss or damage of data) are in place.

Roles and Responsibilities

- **Governing Body:** Holds overall accountability for ensuring the school complies with data protection law.
- **Headteacher:** Acts as the representative of the data controller for day-to-day operations.
- **Data Protection Officer (DPO):** Responsible for monitoring compliance, providing advice, and acting as the point of contact for data subjects and the Information Commissioner's Office (ICO).
- **All Staff:** Responsible for collecting, storing, and processing data in line with this policy.

Individual rights

Under Data Protection Legislation individuals have the right to:

- Access their own personal information within one month of request
- Prevent processing of their information in certain circumstances
- Request that information be corrected, rectified or blocked where it is identified as incorrect
- Expect that we have an officer specifically responsible for data protection in the School

- Expect guidance and training for staff is provided at an appropriate level
- Ensure that any breaches of this policy are dealt with appropriately and in a timely manner.

The Principles of Data Protection

The GDPR stipulates that anyone processing personal data must comply with 6 special categories of good practice. The special categories are legally enforceable. For more information about the special categories, citizens rights and the distinction between personal data and 'special categories' under Data Protection legislation please see the [Information Commissioners Data Protection pages](#).

Legislation and Statutory Guidance

This policy reflects requirements set by:

- **UK General Data Protection Regulation (UK GDPR) & Data Protection Act 2018**
- **Education (Pupil Information) (England) Regulations 2005** (Parental right of access to educational records)
- **Keeping Children Safe in Education (KCSIE)** statutory guidance
- **Department for Education (DfE)** guidance on data protection and generative AI in schools

Data Security & Storage

- **Paper Files:** Safeguarding records, SEN files, and pupil files are stored in locked cabinets with restricted staff access.
- **Digital Files:** Access to Management Information Systems (MIS) is restricted via strong passwords and multi-factor authentication (MFA).
- **Removable Storage:** Staff must not store identifiable pupil data on unencrypted USB sticks or personal devices.

Data Retention and Disposal

Personal data is retained in line with the IRMS (Information and Records Management Society) Toolkit for Schools. Primary school pupil files are securely transferred to the secondary school upon transition or retained until the pupil reaches age 25 where required by law. Shredding and digital wiping are carried out securely.

Data Breaches

A personal data breach involves the accidental or unlawful destruction, loss, alteration, or disclosure of personal data.

- Any suspected breach must be reported immediately to the DPO.
- If a breach poses a high risk to individuals' rights, the DPO will notify the ICO within **72 hours** of awareness and inform affected parents/individuals.

If you would like to know more about how we use your information, please contact Kayleigh Dunn at the school office or our Data Protection Officer at the following address:

Emma Philips

Information Governance Manager
Law and Governance
North Tyneside Council
The Silverlink North
Cobalt Business Park
NE27 0BY

Information, Governance and Compliance
Officer - **Paula Abbott**

email: Information.governance@northtyneside.gov.uk