



Nightingale Primary School

Data Protection Policy

Privacy Notice, as required by the Data Protection Act 2018

Introduction

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (UK GDPR).

Nightingale Primary School collects and uses personal information about staff, pupils, parents, governors, volunteers and other individuals who come into contact with the school. This information is gathered in order to enable the school to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

As a Data Controller, Nightingale Primary School is registered with the Information Commissioner's Office (ICO). Details of the information held and its use are available on the ICO website. The school also has a duty to issue Privacy Notices to staff, pupils and parents, which summarise the information held, why it is held, and the other parties with whom it may be shared.

Purpose

This policy is intended to ensure that personal information is:

- Collected, stored, processed, shared and disposed of correctly and securely.
- Managed in accordance with the Data Protection Act 2018, UK GDPR, and other relevant legislation.
- Protected regardless of the format in which it is held (paper or electronic).

All staff involved with the handling of personal data must understand and follow these guidelines.

What is Personal Information?

Personal data is information that relates to a living individual who can be identified from that data, either directly or indirectly.

Special category data includes sensitive information, such as data relating to health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics, or sexual orientation, and must be handled with additional care.

Data Protection Principles

The UK GDPR sets out six principles (replacing the previous eight) which must be adhered to whenever personal data is processed:

1. **Lawfulness, fairness and transparency** - Data must be processed lawfully, fairly and in a transparent manner.
2. **Purpose limitation** - Data must be collected for specified, explicit and legitimate purposes and not processed in ways incompatible with those purposes.
3. **Data minimisation** - Data must be adequate, relevant and limited to what is necessary.
4. **Accuracy** - Data must be accurate and, where necessary, kept up to date.
5. **Storage limitation** - Data must not be kept for longer than is necessary.
6. **Integrity and confidentiality (security)** - Data must be kept secure, protected against unauthorised or unlawful processing, accidental loss, destruction or damage.

In addition, there is an overarching principle of **accountability**: the school must be able to demonstrate compliance with these principles.

General Statement

The school is committed to maintaining these principles at all times. In practice, this means that the school will:

- Inform individuals why information is being collected at the point of collection.
- Inform individuals when their information is shared, with whom, and for what purpose.
- Ensure the accuracy and quality of the data it holds.
- Retain information only for as long as necessary and securely destroy information that is no longer required.
- Protect personal information from loss, theft, or unauthorised access, regardless of its format.
- Share information only when legally appropriate and in line with data

protection principles.

- Respond promptly and lawfully to Subject Access Requests (SARs) and other data rights requests.
- Ensure that staff are aware of and trained in data protection responsibilities.

Complaints

Complaints regarding data protection will be handled in line with the school's Complaints Policy. Concerns relating to information handling may be referred to the Information Commissioner's Office (ICO), the statutory regulator for data protection.

Review

This policy will be reviewed at least every two years or sooner if required by changes in legislation or guidance. The Headteacher or nominated Data Protection Officer (DPO) will oversee the review.

Contacts

If you have any enquiries relating to this policy, please contact the Headteacher or the school's Data Protection Officer (if applicable).

Further advice and information is available from:

Information Commissioner's Office (ICO)

www.ico.org.uk

Appendix 1 – Procedures for Responding to Subject Access Requests (SARs)

Under the Data Protection Act 2018 and UK GDPR, individuals have the right to access personal data held about them.

Actioning a Subject Access Request (SAR):

1. **Requests** must be made in writing, including via email, and addressed to the Headteacher (or DPO, if applicable). If the request is unclear, the school may request clarification before proceeding.
2. **Identity verification** is required before information is disclosed.
Acceptable proof may include:
 - Passport or driving licence
 - Recent utility bill or council tax statement
 - Birth or marriage certificate
 - P45/P60, mortgage statement or bank/credit card statement
3. **Children and capacity:**
 - A child aged 12 or over is generally presumed to have sufficient understanding to make their own SAR.

- Where a child is deemed competent, their consent is required before releasing their personal data to someone with parental responsibility.
- 4. Fees:**
- Generally, information must be provided free of charge.
 - A reasonable fee may be charged for manifestly unfounded, excessive, or repetitive requests, or for additional copies.
- 5. Response time:**
- The school must respond without undue delay and within **one month** of receipt of the request.
 - This period may be extended by a further two months where requests are complex or numerous (the requester will be informed of the extension and reason within one month).
- 6. Exemptions:**
- Certain information may be withheld if it falls under a legal exemption (e.g., data that would cause serious harm to the physical or mental health of the pupil or another individual, data relating to child protection concerns, or information involving legal proceedings).
- 7. Third-party data:**
- Information relating to another individual will not be disclosed without their consent unless legally appropriate.
- 8. Redaction:**
- If information is redacted, a copy of the full record (with explanations of redactions) will be kept securely in case of future challenges.
- 9. Method of delivery:**
- Information will be provided securely, either electronically, in person, or by recorded delivery, depending on the requestor's preference and security considerations.

Complaints about SARs

Complaints about the handling of Subject Access Requests should be addressed to the Chair of Governors. If unresolved, complaints may be escalated to the ICO.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact the Headteacher.

Date of Policy Approval: Autumn 2025

Date of Next Review: Autumn 2027

