**Windy Nook Primary School**

**Data Protection Policy**

# Aims

The aim of this policy is to ensure that Windy Nook Primary School complies with the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (UK GDPR), and associated legislation. It reflects guidance from the Information Commissioner’s Office (ICO) and outlines the school’s commitment to:

* Protecting the rights and privacy of individuals.
* Ensuring transparency in the collection, use, and storage of personal data.
* Promoting accountability and good data governance.
* Upholding individuals’ rights over their personal data and preventing its misuse.
* Fulfilling the school’s responsibilities as a registered Data Controller with the ICO

# Scope

This policy applies to:

* All staff, governors, volunteers, contractors, consultants, suppliers, and third parties who process personal data on behalf of the school.
* All personal data processed by the school, whether in digital or paper format.
* Any students or staff involved in activities such as research or professional practice that require access to or processing of personal data. In such cases, the relevant school must ensure compliance with data protection laws and refer the activity to the Research Ethics Committee where appropriate.

# Definitions

* **Personal Data:** Information that identifies a living individual.
* **Special Category Data:** Sensitive data such as health, ethnicity, religion, or biometric data.
* **Data Subject:** The individual whose data is being processed.
* **Data Controller:** The school, which determines how and why data is processed.
* **Data Processor:** A third-party processing data on behalf of the school.

# Data Covered by the Policy

This policy applies to all personal data processed by the school, whether held electronically or in paper-based filing systems. Personal data refers to any information that can identify a living individual. It also includes special category data, which requires extra protection.

This includes information about:

* Racial or ethnic origin
* Political opinions
* Religious or philosophical beliefs
* Trade union membership
* Physical or mental health
* Sexual orientation
* Criminal offences or alleged offences, including related proceedings and outcomes

# Legal Framework

This policy complies with:

* UK GDPR
* Data Protection Act 2018
* Education (Pupil Information) (England) Regulations 2005
* ICO guidance and codes of practice

# Roles and Responsibilities

* **Governing Body:** Ensures compliance and oversight.
* **Headteacher:** Implements the policy and ensures staff training.
* **Data Protection Officer (DPO):** Advises on compliance and handles data protection issues.
* **All Staff:** Must understand and follow this policy.

# The Six Data Protection Principles

 We are committed to ensuring that all personal data is processed in accordance with the following principles, as set out in the UK GDPR.

Personal data must be:

1. Processed lawfully, fairly, and transparently – in a way that is open and honest with individuals.
2. Collected for specified, explicit, and legitimate purposes – and not used in a manner incompatible with those purposes.
3. Adequate, relevant, and limited to what is necessary – only the data needed for the intended purpose is collected and used.
4. Accurate and kept up to date – with every reasonable step taken to ensure inaccuracies are corrected or erased promptly.
5. Kept only for as long as necessary – and securely deleted or anonymised when no longer required.
6. Processed securely – using appropriate technical and organisational measures to protect against unauthorised access, loss, or damage.

# Responsibilities

## School ResponsibilitiesThe school has appointed a Data Protection Officer (DPO) to oversee compliance, provide guidance, and manage data protection issues.

## Staff ResponsibilitiesAll staff must:

* Understand and comply with the data protection principles.
* Ensure personal data they handle is accurate, up to date, and securely stored.
* Only use personal data for authorised school-related purposes.
* Obtain appropriate consent when collecting, sharing, or disclosing personal data.
* Complete mandatory data protection training during induction and refresher sessions regularly.
* Report any concerns or uncertainties to the DPO or the designated contacts, Lucie Forrest & Michelle Gerry.

## Student ResponsibilitiesStudents must:

* Follow the school’s data protection principles.
* Comply with any security procedures in place.

# Collecting, Using, and Sharing Personal Data

We are committed to collecting and handling personal data responsibly, lawfully, and transparently. The school only collects personal data that is necessary for specific, legitimate purposes, including:

* Delivering education and safeguarding pupils.
* Managing staff employment and school administration.
* Meeting legal and statutory obligations.

Where required, consent is obtained—particularly for the use of photographs, videos, and participation in optional services.

## Obtaining and Using Data

* Personal data is collected only when necessary for a defined school-related purpose.
* Students and staff are informed about how their data will be processed at the point of registration or employment.
* All data must be collected and stored securely, in line with the school’s data protection and information security policies.

## Disclosing and Sharing Data

All data sharing requests relating to national security, crime, or taxation must be referred to the designated Data Protection Officer, Lucie Forrest.

* Personal data will not be disclosed to third parties without the individual’s prior consent, unless required by law.
* This includes confirming whether someone is or has been a student, applicant, or employee.
* The school may be legally required to share data with authorised bodies (e.g. police, safeguarding agencies, or law enforcement) under the Data Protection Act 2018.
* Regular data sharing with third parties is governed by written agreements that define the scope and safeguards.
* Ad hoc data sharing must also comply with legal requirements and be proportionate, secure, and documented.

# Data Sharing

The school is committed to sharing personal data responsibly and in compliance with the Data Protection Act 2018 and UK GDPR. All data sharing must be documented and, where appropriate, referred to the Data Protection Officer for guidance.

Key principles include:

* **Purpose Limitation:** Personal data is only collected and shared when necessary for a specific, legitimate school-related purpose.
* **Transparency:** Students and staff are informed about how their data will be used at the point of registration or employment.
* **Consent:** Personal data will not be disclosed to third parties without the individual’s prior consent, unless legally required.
* **Legal Obligations:** The school may share data with authorised bodies (e.g. police, safeguarding authorities) where required by law.
* **Agreements:** Regular data sharing with third parties is governed by written agreements outlining the scope and safeguards.
* **Ad Hoc Sharing:** Occasional data sharing must still comply with legal requirements and be justified, proportionate, and secure.

# Transferring Personal Data

The school ensures that all transfers of personal data are carried out securely and in accordance with the school’s Information Security Policy.

The following practices apply:

* Secure Transfers: Personal data must only be transferred using secure methods that comply with school policy.
* Email Security: External email should be avoided for sending personal data unless the message is encrypted and the password is shared separately (e.g. by phone).
* Recipient Verification: Staff must double-check recipient addresses before sending emails containing personal data. Care should be taken when using “reply all,” forwarding, or copying others into emails.
* Use of BCC: When emailing multiple recipients, the blind copy (BCC) function should be used to prevent accidental disclosure of personal information.
* Prohibited Use of Personal Accounts: Staff must not use personal email accounts to send or receive personal data for school-related purposes.

# Data Subject Rights

* Under the UK GDPR, individuals have the following rights regarding their personal data:
* Right of Access – to request and receive a copy of their personal data.
* Right to Rectification – to correct inaccurate or incomplete data.
* Right to Erasure – to request deletion of data in certain circumstances.
* Right to Restrict Processing – to limit how their data is used.
* Right to Object – to object to processing based on legitimate interests or for direct marketing.
* Right to Data Portability – to receive their data in a structured, commonly used format and transfer it to another controller.

All requests must be made in writing to the Data Protection Officer (DPO). The school will respond within one calendar month, in line with statutory requirements.

# Retention, Security and Disposal

We are committed to ensuring that personal data is accurate, securely stored, and retained only for as long as necessary. The following principles apply:

* **Accuracy and Updates:** Staff responsible for managing personal data must ensure it is accurate and up to date. Any concerns about data accuracy should be reported to the Data Protection Officer (e.g. Lucie Forrest).
* **Retention Periods:** Personal data, whether in paper or electronic format, must not be kept longer than necessary. Data is retained only for business, legal, or regulatory purposes in line with the school’s Retention Schedule.
* **Secure Storage:** All staff must take personal responsibility for the secure storage of data. Appropriate measures must be in place to prevent loss, damage, or unauthorised access.
* **Remote Working:** Staff working from home must ensure that personal data is stored securely and is not accessible to others, in accordance with the school’s Flexible Working Scheme.
* **Secure Disposal:**
* Paper records must be shredded or placed in confidential waste bins.
* Electronic data must be securely deleted.
* CDs, USB drives, and other media must be passed to the IT provider for safe disposal.
* Hardware must be degaussed or disposed of in line with IT service provider contracts and data protection regulations.

# Data Security and Breaches

The school implements appropriate technical and organisational measures to protect personal data from unauthorised access, loss, or damage. These include secure storage systems, access controls, staff training, and regular reviews of data handling practices.

In the event of a data breach:

* The breach must be reported immediately to the Data Protection Officer (DPO).
* If the breach poses a risk to individuals’ rights and freedoms, it will be reported to the Information Commissioner’s Office (ICO) within 72 hours.
* Affected individuals will be informed where there is a high risk to their rights and freedoms.
* All breaches will be investigated and documented in accordance with the school’s Data Breach Policy.

# Training and Awareness

The school ensures that data protection remains a core part of its organisational culture. All staff receive regular training on their data protection responsibilities.

This includes:

* Mandatory training during induction for new staff.
* Periodic refresher training to ensure continued awareness of data protection principles and procedures.
* Guidance on recognising and reporting data breaches, handling personal data securely, and respecting individuals’ rights.

# Monitoring and Review

This policy is reviewed annually or in response to significant changes in legislation or school operations.