

Data Protection & GDPR Policy

This policy was updated: **September 2025**

This policy will be reviewed: **September 2026**

Statutory policy? **Yes**

Index

1. Aims
2. Legislation and Guidance
3. Definitions
4. Data Protection Principles
5. Roles and Responsibilities
6. Lawful Basis for Processing
7. Categories of Data Processed
8. Data Storage and Security
9. Data Sharing
10. Data Retention
11. Data Requests and Information Sharing
12. Data Subject Rights
13. Data Breaches
14. Training and Awareness
15. Monitoring and Review
16. Compliance Statement
17. Complaints
18. Contact Us

1. Aims

Nulogic is committed to protecting the rights and freedoms of individuals in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy sets out how the school manages personal data in a clear, lawful, and secure manner.

It is designed to ensure all staff understand both their responsibilities and the expectations placed upon them when handling personal information within an educational setting.

2. Legislation and Guidance

This policy is based on key legislation and statutory guidance that governs how schools must manage data. These include:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Education (Pupil Information) Regulations
- Keeping Children Safe in Education (KCSIE)
- Information Commissioner's Office (ICO) guidance

Staff are expected to have a basic awareness of these requirements and understand how they apply in practice.

The school ensures that data protection supports safeguarding and promotes the welfare of learners at all times.

3. Definitions

For clarity, the following definitions apply throughout this policy.

Personal Data refers to any information relating to an identified or identifiable individual. This includes names, addresses, dates of birth, and contact details.

Special Category Data is more sensitive and requires additional protection. This includes information such as health, safeguarding records, ethnicity, and SEN/EHCP details.

Processing refers to any action taken with data, including collecting, storing, using, sharing, or deleting it.

4. Data Protection Principles

Nulogic follows the seven core principles of GDPR. These principles underpin all data handling within the school and must be applied in day-to-day practice.

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

In practice, this means staff should always be clear on why they are using data, only use what is necessary, and ensure it is handled securely at all times.

5. Roles and Responsibilities

Clear roles are in place to ensure accountability across Nulogic:

- The Headteacher holds overall responsibility for ensuring the school meets its data protection obligations and that appropriate systems and procedures are in place.
- The Data Protection Lead/DPO oversees compliance, manages data breaches and requests, and provides guidance to staff where needed.
- The Designated Safeguarding Lead (DSL) is responsible for the oversight of safeguarding records and ensuring that highly sensitive information is handled appropriately and securely.

All staff, regardless of role, are responsible for handling data correctly and reporting any concerns immediately.

6. Lawful Basis for Processing

The school must have a lawful basis for all data it processes. In most cases, this will be linked directly to its role as an education provider.

Nulogic processes data under the following bases:

- Public task – delivering education and support to learners.
- Legal obligation – including safeguarding, attendance, and statutory duties.
- Vital interests – where there is a need to protect a child or individual.
- Consent – for specific purposes such as photographs or non-essential information.

Staff should not assume data can be shared or used without considering the lawful basis first.

7. Categories of Data Processed

As part of its day-to-day operation, the school processes a range of information relating to learners, staff, and families.

This includes:

- Learner details such as name, date of birth, and address
- Attendance, behaviour, and progress data
- Safeguarding and welfare records
- SEN and EHCP information
- Medical and health-related information where required
- Staff employment records
- Parent and carer contact details

Only data that is necessary for the school to function effectively will be collected and used.

8. Data Storage and Security

Nulogic takes data security seriously and has measures in place to ensure information is protected at all times. The school uses secure systems such as CPOMS for safeguarding and Microsoft Teams for operational processes. Access to these systems is controlled, monitored, and regularly reviewed to ensure compliance and identify any risks.

Key expectations for staff include:

- Keeping passwords secure and not sharing login details
- Locking devices when unattended
- Ensuring confidential information is not left visible
- Only accessing data that is relevant to their role

Paper records must be stored in locked cabinets, and any transfer of information must be carried out securely.

9. Data Sharing

Nulogic regularly works with external agencies and may need to share information to support learners effectively.

Data may be shared with:

- Local Authorities and other relevant statutory agencies
- Schools and education providers
- Safeguarding partners
- External professionals such as social workers or police

All data sharing is lawful, necessary, proportionate and recorded appropriately, with safeguarding taking priority where applicable.

10. Data Retention

Nulogic follows recognised retention guidance, including the Information and Records Management Society (IRMS) Toolkit for Schools, to ensure that data is retained only for as long as necessary and disposed of securely when no longer required.

- Learner records are retained until date of birth + 25 years
- Safeguarding records follow the same retention period
- Attendance registers are kept for a minimum of 3 years
- Staff records are retained in line with employment law

Once retention periods expire, data is securely destroyed.

11. Data Requests and Information Sharing

The school may receive formal requests for personal data from external agencies. These requests are managed carefully to ensure compliance with UK GDPR and the Data Protection Act 2018.

All requests must:

- Be submitted in writing using a recognised data request form
- Clearly state the purpose of the request
- Specify the exact data required

This includes Subject Access Requests (SARs), which will be processed in accordance with statutory timescales.

When a request is received, the school will review the information provided and assess whether it is lawful and appropriate to share.

This includes:

- Confirming the request is necessary and proportionate
- Ensuring there is a valid lawful basis
- Applying the principle of data minimisation

Where needed, further clarification will be sought before any information is released. All data shared will be transferred securely and recorded to maintain a clear audit trail.

If a request does not meet requirements, it may be refused or delayed in line with statutory guidance.

Records of all requests and disclosures are maintained to demonstrate accountability and compliance.

12. Data Subject Rights

Individuals have specific rights under GDPR, and the school must ensure these are upheld. These include the right to:

- Access their personal data
- Request corrections to inaccurate information
- Request deletion where applicable
- Restrict or object to processing

Requests must be handled promptly and responded to within one month.

13. Data Breaches

A data breach is any incident where personal data is lost, accessed without authorisation, or disclosed incorrectly. All staff have a responsibility to report concerns immediately. Nulogic has a structured response process in place. This includes:

- Completing a formal Data Breach Reporting Template
- Recording incidents within a Data Breach Register
- Escalating concerns to the Data Protection Lead

The process requires clear recording of what happened, the data involved, and the actions taken. The Data Protection Lead will assess the situation, determine risk, and decide whether the breach must be reported to the ICO within 72 hours. All breaches are reviewed to identify patterns and improve future practice.

14. Training and Awareness

All staff receive data protection training as part of their role. This ensures they understand both their responsibilities and how data protection links directly to safeguarding. Ongoing updates and reminders will be provided where needed.

15. Monitoring and Review

This policy is reviewed annually and updated in response to changes in legislation, guidance, or school practice. The school ensures that this policy is actively implemented and understood by staff, and that practice reflects the expectations set out within it.

16. Compliance Statement

Failure to follow this policy may result in disciplinary action. Nulogic expects all staff to uphold high standards when handling personal data and to act in a way that protects the rights and safety of all individuals.

Failure to comply may also result in referral to external regulatory bodies where appropriate.

17. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us at any time by contacting Bradley Reece-Jones at breece-jones@nulogictraining.co.uk

Alternatively, you can make a complaint at any time to the Information Commissioner's Office:

Report a concern online at <https://ico.org.uk/make-a-complaint/>

Call 0303 123 1113

Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

18. Contact us

If you have any questions or concerns, or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

Bradley Reece-Jones at breece-jones@nuloqictraining.co.uk