Data Protection & GDPR Guidelines 2026

Introduction

Grangemockler NS is committed to protecting the personal data of pupils, parents/guardians, and staff in line with the General Data Protection Regulation (GDPR, EU 2018) and the Data Protection Acts 1988–2018.

These guidelines outline how the school collects, stores, uses, and shares personal data, and ensure that all stakeholders understand their rights and responsibilities.

Data Controller

The Board of Management (BoM) of Grangemockler NS is the data controller. The Principal acts on behalf of the BoM in relation to data protection matters.

Contact:

- Principal: Mr. Stephen Hahessy
- Email: school@grangemocklerns.ie
- Phone: 051 647222

What Personal Data We Process

The school collects and processes personal data necessary for education, welfare, and administration, including:

- Pupils: name, address, date of birth, contact details, PPS number, attendance, assessment results, SEN records, medical information, photographs (with consent).
- Parents/Guardians: contact details, financial details (re fees, voluntary contributions, etc.).
- Staff: contact details, qualifications, vetting, payroll information.

Legal Basis for Processing

The school processes personal data based on:

- Legal obligation (e.g., Department of Education returns, Tusla attendance reporting).
- Public interest (providing education).
- Contractual necessity (employment contracts).
- Consent (e.g., publishing photos on school website, use of apps/platforms).

Data Protection Principles

The school ensures that personal data is:

1. Processed lawfully, fairly, and transparently.
2. Collected for specified, legitimate purposes.
3. Adequate, relevant, and limited to what is necessary.
4. Accurate and kept up to date.
5. Retained only for as long as necessary, respective to role.
6. Stored securely to ensure confidentiality and integrity.

Data Storage & Security

- Paper records (e.g., enrolment forms, assessment results) are stored securely in locked cabinets.
- Digital data is stored on password-protected systems with regular backups.
- Main School devices are encrypted and password-protected.
- Access to pupil and staff data is restricted to authorised personnel only.
- Aladdin and Google Workspace are used in compliance with GDPR.

Sharing of Data

Personal data may be shared with third parties only when legally required or when necessary for education and welfare. Examples include:

- Department of Education & Skills (returns, inspections).
- Tusla (attendance and child protection).
- HSE (immunisation, speech & language, assessments).
- NCSE / NEPS (educational support services).
- BOM-approved online platforms (with parental consent).

The school does not share personal data with third parties for commercial purposes.

Photographs, Video & Digital Platforms

- Parental consent will be obtained before publishing pupil photos, work, or videos online.

- Pupils will be identified by first name only (or not at all).
- Staff will ensure that all apps, websites, and platforms used for teaching are GDPR compliant.
- Parents may withdraw consent at any time by contacting the school in writing, in this instance permission will be asked to cover faces rather than excluding them from photographs.

Data Retention

The school follows Department of Education and Data Protection Commission guidance on retention:

- Pupil records – kept until pupil is 21 years of age.
- Child protection records – retained indefinitely.
- Staff records – retained for the duration of employment + statutory period.
- Financial records – retained for at least 7 years.

Rights of Data Subjects

Pupils, parents, and staff have the right to:

- Access their personal data held by the school.
- Request correction of inaccurate data.
- Request erasure (where applicable).
- Restrict or object to processing (in certain cases).
- Data portability (where applicable).

Requests should be made in writing to the Principal.

Data Breaches

In the event of a data breach:

- The Principal will inform the Data Protection Commission within 72 hours (if required).
- The affected individuals will be notified where there is a high risk to their rights or freedoms.
- The BOM will review procedures to prevent recurrence.

Roles & Responsibilities

- Board of Management – overall responsibility for data protection compliance.
- Principal – day-to-day management of GDPR compliance.
- Staff – ensure personal data is handled securely and responsibly.
- Parents/Pupils – respect school guidelines when handling digital information.

Communication & Training

- Staff to receive training on GDPR and data protection practices.
- Parents will be informed of policies at enrolment and through the school website.
- The AUP and ICT Policy work alongside this document to ensure compliance.

Review & Ratification

This policy was adopted by the Board of Management of Grangemockler NS on: 11/2/2026

Signed: _____ (Chairperson, BOM)

Signed: _____ (Principal)

Signed: Vera Power (Teacher Responsible)

Review date: December 2028