BURLINGTON INFANT AND NURSERY SCHOOL

POLICY TITLE: General Data Protection Regulations

Persons with Responsibility: School Business Manager

Data Protection Officer: Erris Business Management (admin@ebm-services.co.uk)

Key Legislation:
Freedom of Information Act 2000
The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
The School Standards and Framework Act 1998
The UK General Data Protection Regulation and the Data Protection Act 2018
The Data Protection and Digital Information Act 2024 (DPDI Act)

Documents consulted:
Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)
Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
Information Commissioner's Office (2021) 'The UK GDPR'

Associated School Policy:
Photography and Mobile phones (From Safeguarding Policy)
E-safety Policy
Freedom of Information Policy

Policy History:

Issue No.	Date	Author	Summary of Changes	Next Review Date
5	Sept 23	CB	Reviewed, no changes	September 2024
6	Sept 24	CB	Reviewed	September 2025
7	Jan 2026	SYW	Updated	Spring 2027

Approved by Governors at a meeting on : _____

Please refer to signed minutes of this meeting

1. Statement of intent

The school is required to process personal information about staff, pupils, families, and contractors to meet legal obligations. This policy ensures all staff and governors understand their responsibilities and comply with the **UK GDPR** and **Data Protection Act 2018**.

2. Applicable data

2.1. **Personal data:** Information relating to an identifiable living individual, including online identifiers like IP addresses.

2.2. **Special category data:** Sensitive data such as ethnic origin, health, sexual orientation, religious or philosophical beliefs, biometric, or genetic data.

2.3. **Criminal offence data:** Processed only under official authority or when authorised by domestic law.

2.4. The school holds personal data relating to:

- children - for educational, welfare and safeguarding reasons
- employees - for payroll, employment, HR, administrative reasons
- parents - for contact and administrative reasons

2. Principles

2.1 Personal data will be:

- Processed lawfully, fairly, and transparently.
- Collected for specified, explicit, and legitimate purposes.
- Adequate, relevant, and limited to what is necessary (**data minimisation**).
- Accurate and kept up to date.
- Kept no longer than necessary.
- Processed securely.

2.2 The school remains accountable and able to demonstrate compliance.

3. Accountability and Governance

3.1 The School will implement appropriate technical and organisational measures to demonstrate compliance.

3.2 The school will provide comprehensive, clear and accessible privacy policies.

3.3 Records of processing activities (ROPAs) are maintained where processing is high risk. e.g. the processing of special categories data or that in relation to criminal convictions and offences.

3.4 Internal records of processing activities will include the following:

- Name and details of the organisation (controller details)
- Purposes of the processing
- Categories of data subjects and data
- Retention periods
- Security measures

3.5 Data protection by design and by default is embedded in all processing activities.

3.6 Data Protection Impact Assessments (DPIAs) are completed where required.

4. Data Protection Officer (DPO)

4.1 The school has a DPO assigned by a compliance management company.

- The DPO advises on compliance - Monitors data protection practices, conducts internal audits. Acts as the contact point with the ICO
- The DPO reports to the School Business Manager and Headteacher and operates independently.
- The DPO monitors the school's compliance with the GDPR and other laws annually and as and when required.

5. Lawful processing

5.1 A lawful basis is identified and documented before processing data. Lawful bases include:

5.2 Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
    - Legal obligation
    - Public task
    - Contract and employment
    - Vital interests
    - Consent

5.3 Sensitive data, e.g SEND, health, safeguarding will only be processed under the following conditions:

- It is **necessary for education, safeguarding or welfare** (public task) AND it's allowed under Article 9 because:
- It is required by education or safeguarding law
- It is necessary for health or social care
- It is in the substantial public interest

6. Consent

6.1 Consent is freely given, specific, informed and unambiguous.

6.2 Silence or pre-ticked boxes do not constitute consent.

6.3 Records of consent are maintained.

6.4 Consent can be withdrawn at any time.

6.5 Consent of parents for children under the age of 16 will be sought prior to the processing of their data, except where the processing is related to safeguarding.

7. Individual rights

- Right to be informed
- Right of access: a ‘reasonable fee’ to comply with requests may be charged
- Right to rectification
- Right to erasure: where consent is withdrawn, where the data is no longer necessary. The right to erasure cannot be exercised if the data is related to safeguarding, SEND, attendance, or to meet statutory requirements
- Right to restrict processing
- Right to data portability
- Right to object

7.1 Where a request is unfounded or excessive, the school holds the right to refuse to respond to the request.

8. Subject Access Requests (SARS)

8.1 Requests are responded to within one month (or two months for complex cases)

8.2 Extensions of up to two months apply where requests are complex.

8.3 The term ‘reasonable fee’ applies only to excessive or unfounded requests, not routine SARS.

9. Automated Decision-Making and AI

9.1 The school does not use Generative AI for decision-making regarding grading, behaviour sanctions, admissions, staff appraisals without human review.

9.2 If this changes, individuals will be informed and appropriate safeguards applied.

10. Use of Generative AI (New)

10.1 Staff and pupils must not input personal or sensitive data into generative AI platforms unless a full DPIA has been approved.

10.2 Only AI systems assessed for security and transparency will be used.

10.3 Any AI-related breaches must be reported to the DPO immediately.

11. Data breaches

11.1 ‘Personal data breaches’ are reported internally without delay. Advice will be sought from the DPO and/or ICO where appropriate.

11.2 Breaches posing a risk to individuals’ rights and freedoms are reported to the ICO within 72 hours.

11.3 High-risk breaches are communicated to affected individuals.

12. Data security

12.1 Physical, technical and organisational security measures are in place.

- Digital**:** Password protection, encryption, and remote blocking/deletion for mobile devices are used.
- Emails: Sensitive info is password-protected.
- Mobile Devices: Staff using laptops and tablets for work must ensure they are encrypted and approved by the school.

12.2 Two-factor authentication, encryption, password protection and access controls are used.

12.3 Cyber security measures are reviewed annually in line with Cyber security training and requirements.

12.4 Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.

13. Data Retention

13.1 Data is kept only as long as necessary, aligned with DfE,ICO and IRMS toolkit guidance.

13.2 Disposal: Paper is shredded; digital storage is physically destroyed or scrubbed.

14. Publication and photography

14.1 Personal data is not published without appropriate consent.

14.2 Safeguarding considerations apply to all images and video.

15. DBS and Employment data

15.1 DBS data is processed securely and not retained longer than necessary.

15.2 Access is strictly limited.

16. Policy review

16.1 This policy is reviewed annually by the SBM and the headteacher.

Next review date: is Spring 2027.