Data Protection (GDPR) Policy Document

Date of policy: February 2023
Date approved by Governing Body: 10.3.23
Review date: February 2024

Data Protection (GDPR) Policy

The following policy relates to all Brinscall St John's CE/Methodist Primary School. employees (including voluntary, temporary, contract and seconded employees), who capture, create, store, use, share and dispose of information on behalf of Brinscall St John's CE/Methodist Primary School.

These persons shall be referred to as 'Users' throughout the rest of this policy.

Brinscall St John's CE/Methodist Primary School shall be referred to as 'the school' or 'we' throughout the rest of this policy.

The following policy relates to all electronic and paper based information.

Statement of Commitment

In order to undertake our statutory obligations effectively, deliver services and meet customer requirements, the school needs to collect, use and retain information, much of which is personal, sensitive or confidential.

Such information may be about:

- Pupils.
- Parents and Guardians.
- Governors.
- Employees or their families.
- Members of the public.
- Business partners.
- Local authorities or public bodies.

We regard the lawful and correct treatment of personal data by the school as very important to maintain the confidence of our stakeholders and to operate successfully.

To this end, the school will ensure compliance, in all its functions, with the Data Protection Act (DPA) 1998, the UK General Data Protection Regulation (UK GDPR) and the new Data Protection Act (DPA) 2018, School Standards and Framework Act 1988, Freedom of Information Act 2000; Electronic Commerce (EC Directive) Regulations 2002; The Privacy and Electronic Communications (EC Directive) Regulations 2003 and with other relevant legislation.

This policy also operates in conjunction with school policies including (but not exclusively): Child Protection and Safeguarding Policy.

Data Protection Principles

The Principles of DPA and GDPR state that personal information must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals; the lawful basis can be:

- Consent of a data subject;
- Processing is necessary for the performance of a contract with the data subject;
- Processing is necessary for compliance with a legal obligation (e.g. The Education Act 1996, School Standards and Framework Act 1998, Education Act 2002, Children and Families Act 2014);
- Processing is necessary to protect the vital interests of the data subject or another person (e.g. life or death);
- Processing is necessary for the performance of a task carried out in the public interest.

The lawful basis for sensitive personal data (racial, political, religious, trade union, genetic, health, sex life, criminal convictions or offences) is:

- Explicit consent of the data subject;
- Processing is necessary for carrying out obligations under employment, social security or social protection law;
- Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent;
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members and provided there is no disclosure to a third party without consent;
- Processing relates to personal data manifestly made public by the data subject;
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest;
- Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services;
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal

products or medical devices;

- Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. Accurate and, where necessary, kept up to date;

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6. Processed in a manner that ensures appropriate security of the personal data against unauthorised processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

Compliance with the Data Protection Principles and Data Protection Legislation

In order to comply with these principles and meet all data protection obligations as stipulated in data protection legislation, the school will:

- Raise awareness of data protection across the school;
- Offer data protection training to all employees and governors;
- Create a data protection policy for the school that is updated annually;
- Complete a personal data processing audit, which lists the following:
    - Name of the personal data set;
    - Purpose for processing this personal data set;
    - Who the data set is shared with;
    - Whether the data transferred to another country;
    - How long the personal data set is kept (retention);
    - The technical and organisational security measures to protect the personal data set;
    - The legal basis for processing as described above (1);
    - If consent is the legal basis for processing, details of the evidence of this consent.
- Put any risks found from the personal data processing audit process into a risk register.
- Review the school's consent forms so they meet the higher standards of GDPR, create an audit trail showing evidence of consent.
- Under 13's can never themselves consent to the processing of their personal data in relation to online services, this rule is subject to certain exceptions such as counselling services.

- Register with the Information Commissioners Officer as a data controller.
- Appoint a data protection officer who will monitor compliance with the GDPR and other data protection laws.
- Create a privacy notice that will let individuals know who we are, why we are processing their data and if we share their data.
- Create a system to allow data subjects to exercise their rights:
    - Right to be informed via a privacy notice;
    - Right of access via a subject access request within 1 month;
    - Right of rectification to incorrect data within 1 month;
    - Right to erasure unless there is a legal reason for processing their data;
    - Right to restrict processing to the bare minimum;
    - Right to data portability to receive their data in the format they request;
    - Right to object to personal data being used for profiling, direct marketing or research purposes;
    - Rights in relation to automated decision making and profiling.
- Amend any business contracts with suppliers to ensure that they will conform to new data protection legislation.
- Implement technical and organisational controls to keep personal data secure.
- Use Privacy Impact Assessments to assess the privacy aspects of any projects or systems processing personal data.
- Ensure an adequate level of protection for any personal data processed by others on behalf of the school that is transferred outside the European Economic Area.
- Investigate all information security breaches, and if reportable, report to the Information Commissioners Office within 72 hours.
- Undertake data quality checks to ensure personal data is accurate and up to date.
- Demonstrate our compliance in an accountable manner through audits, spot checks, accreditations and performance checks.
- Support the pseudonymisation and encryption of personal data.

Data breaches

The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The headteacher will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Where the school faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Within a breach notification to the supervisory authority, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Where notifying an individual about a breach to their personal data, the school will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

The school will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

The school will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

Cloud Computing

For the purposes of this policy, **'cloud computing'** refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the school accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

All files and personal data will be encrypted before they leave a school device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

As with files on school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the school's policies for the use of cloud computing.

The school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the school's Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk.
- Monitor the use of the school's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the headteacher

Rights of the Individual

The list of rights that a data subject (person who the data is about) can exercise has been widened by Section 2 of the GDPR:

- The right to be informed; via privacy notices.

- The right of access; via subject access requests (SARS), the timescale for response has been reduced from 40 calendar days to one calendar month. SARs must be free of charge, charges can only be made for further copies or where requests for information are unfounded or excessive.
- The right of rectification; inaccurate or incomplete data must be rectified within one month.
- The right to erasure; individuals have a right to have their personal data erased and to prevent processing unless we have a legal obligation to do so.
- The right to restrict processing; individuals have the right to suppress processing. We can retain just enough information about the individual to ensure that the restriction is respected in future.
- The right to data portability; we need to provide individuals with their personal data in a structured, commonly used, machine readable form when asked.
- The right to object; individuals can object to their personal data being used for profiling, direct marketing or research purposes.
- Rights in relation to automated decision making and profiling; GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

The school will ensure that these rights will be exercised.

Contact

Contact the Data Protection Officer by:

Email: bursar@brinscall.lancs.sch.uk

Phone: 01254 830700

Post: Brinscall St John's CE/Methodist Primary School, Harbour Lane, Brinscall, Chorley, PR6 8PT

Version Control

Named Owner:	C Lormor – Data Protection Officer
Version Number:	2.00
Date Of Creation:	June 2018
Last Review:	February 2023
Next Scheduled Review:	February 2024
Overview of Amendments to this Version:	updated legislation, Addition of sections for: Cloud Computing and Data breaches as per new guidance.