Much Birch C of E Primary School

Data Protection Policy / GDPR



'We will flourish and reach our God given potential'

I am the vine; you are the branches. If you remain in me and I in you, you will bear much fruit. John 15:5

All members of our whole school community are able to realise their God-given potential, enabling them to become equal, caring and active citizens whilst upholding true Christian values. We treat others, as we would like to be treated, with dignity and respect. Everyone is encouraged to flourish with hope and high aspirations

DATA PROTECTION POLICY

1. Introduction

MUCH BIRCH School has a responsibility under the Data Protection Act 2018 to hold, obtain, record, use and store all personal data relating to an identifiable individual in a secure and confidential manner. This Policy is a statement of what the School does to ensure its compliance with the Act.

The Data Protection Policy applies to all School employees, governors, volunteers, and contractors. The Policy provides a framework within which the School will ensure compliance with the requirements of the Act and will underpin any operational procedures and activities connected with the implementation of the Act.

2. Background

The Data Protection Act 2018 governs the handling of personal information that identifies living individuals directly or indirectly and covers both manual and computerised information. It provides a mechanism by which individuals about whom data is held (the "data subjects") can have a certain amount of control over the way in which it is handled.

Some of the main features of the Act are:

- All data covered by the Act must be handled in accordance with the Six Data Protection Principles (see Appendix 1)

- The person about whom the information is held (the Data Subject) has various rights under the Act including the right to be informed about what personal data is being processed, the right to request access to that information, the right to request that inaccuracies or incomplete data are rectified, and the right to have personal data erased and to prevent or restrict processing in specific circumstances. Individuals also have the right to object to processing based on the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling); and processing for the purposes of scientific/historical research and statistics. There are also rights concerning automated decision making (including profiling) and data portability.

- Processing of special categories of data must be done under a lawful basis. This data includes information about race, ethnic origin, political persuasion, religious belief, trade union membership, genetics, biometrics (where used for identification purposes), health, sex life and sexual orientation.

- The Data Protection Act deals with criminal offence data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.

- There is a principle of accountability of data controllers to implement appropriate technical and organisational measures that include internal data protection policies and procedures, staff training and awareness of the requirements of the Act, internal audits of processing activities, maintaining relevant documentation on processing activities, appointing a data protection officer, and implementing measures that meet the principles of data protection by design and data protection by default, including data minimisation, transparency, and creating and improving security features on an ongoing basis.

- Data protection impact assessments are carried out where appropriate as part of the design and planning of projects, systems and programmes.

- Data controllers must have written contracts in place with all data processors and ensure that processors are only appointed if they can provide 'sufficient guarantees' that the requirements of the Act will be met and the rights of data subjects protected.

- Data breaches that are likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office within 72 hours of the school becoming aware of the breach. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the school will notify those individuals concerned directly.

- The Information Commissioner is responsible for regulation and issue notices to organisations where they are not complying with the requirements of the Act. She also has the ability to prosecute those who commit offences under the Act and to issue fines.

3 Policy Statement

The School is committed to ensuring that personal information is handled in a secure and confidential manner in accordance with its obligations under the Data Protection Act 2018 and professional guidelines. The School will use all appropriate and necessary means at its disposal to comply with the Data Protection Act and associated guidance.

4 Roles and Responsibilities

4.1 Data Protection Officer

The Data Protection Officer is Bernadette Davies (Head teacher), and they are responsible for the following tasks:

- informing and advising the school, any processor engaged by the school as data controller, and any employee of the school who carries out processing of personal data, of that person's obligations under the legislation
- providing advice and monitoring for the carrying out of a data protection impact assessment
- co-operating with the Information Commissioner's Office,
- acting as the contact point for the Information Commissioner's Office
- monitoring compliance with policies of the school in relation to the protection of personal data
- monitoring compliance by the school with the legislation.

In relation to the policies mentioned above, the data protection officer's tasks include—

(a) assigning responsibilities under those policies,

(b) raising awareness of those policies,

(c) training staff involved in processing operations, and

(d) conducting audits required under those policies.

The school must provide the Data Protection Officer with the necessary resources and access to personal data and processing operations to enable them to perform the tasks outlined above and to maintain their expert knowledge of data protection law and practice.

4.2 School

The School will be responsible for ensuring that the organisation complies with its responsibilities under the Data Protection Act through monitoring of activities and incidents via reporting by the Data

Protection Officer. The School will also ensure that there are adequate resources to support the work outlined in this policy to ensure compliance with the Data Protection Act.

4.3 All Staff and Governors

All staff and governors will ensure that:-

- Personal information is treated in a confidential manner in accordance with this and any associated policies.
- The rights of data subjects are respected at all times.
- Privacy notices will be made available to inform individuals how their data is being processed.
- Personal information is only used for the stated purpose, unless explicit consent has been given by the Data Subject to use their information for a different purpose.
- Personal information is only disclosed on a strict need to know basis, to recipients who are entitled to that information.
- Personal information held within applications, systems, personal or shared drives is only accessed in order to carry out work responsibilities.
- Personal information is recorded accurately and is kept up to date.
- They refer any subject access requests and/or requests in relation to the rights of individuals to the Data Protection Officer.
- They raise actual or potential breaches of the Data Protection Act to the Data Protection Officer as soon as the breach is discovered.

It is the responsibility of all staff and governors to ensure that they comply with the requirements of this policy and any associated policies or procedures.

4.9 Contractors and Employment Agencies

Where contractors are used, the contracts between the School and these third parties should contain mandatory information assurance clauses to ensure that the contract staff are bound by the same code of behaviour as school members of staff and governors in relation to the Data Protection Act.

4.10 Volunteers

All volunteers are bound by the same code of behaviour as school members of staff and governors in relation to the Data Protection Act.

5 Records Management

Good records management practice plays a pivotal role in ensuring that the school is able to meet its obligations to provide information, and to retain it, in a timely and effective manner in order to meet the requirements of the Act. All records should be retained and disposed of in accordance with the School retention schedule.

6 Consent

The school will take all reasonable steps to ensure that service users, members of staff, volunteers, and contractors are informed of the reasons the school requires information from them, how that information will be used and who it will be shared with. This will enable the data subject to give explicit informed consent to the school handling their data where the legal basis for processing is consent.

Should the school wish to use personal data for any purpose other than that specified when it was originally obtained, the data subject's explicit consent should be obtained prior to using the data in the new way unless exceptionally such use is in accordance with other provisions of the Act.

Should the school wish to share personal data with anyone other that those recipients specified at the time the data was originally obtained, the data subject's explicit consent should be obtained prior to sharing that data, failure to do so could result in a breach of confidentiality.

7 Accuracy and Data Quality

The school will ensure that all reasonable steps are taken to confirm the validity of personal information directly with the data subject.

All members of staff and governors must ensure that service user personal information is checked and kept accurate and up to date on a regular basis, for example, by checking it with the service user when they attend for appointments in order that the information held can be validated.

Where a member of the public exercises their right for their data to be erased, rectified, or restricted, or where a member of the public objects to the processing of their data, the Data Protection Officer must be notified and the appropriate procedures followed.

8 Data Protection Impact Assessments

A data protection impact assessment is a process which helps to assess privacy risks to individuals in the collection, use and disclosure of information. They must be carried out at the early stages of projects and are embedded in to the school's decision making process.

9 Providers

The school must have written contracts in place with all suppliers who process personal data on behalf of the school as "data processors". The school will ensure that processors are only appointed if they can provide 'sufficient guarantees' through the procurement process that the requirements of the Act will be met and the rights of data subjects protected.

10 Complaints

Any expression of dissatisfaction from an applicant with reference to the school's handling of personal information will be treated as a complaint, and handled under the school's complaint's processes. The Data Protection Officer will be involved in responding to the complaint.

Should the complainant remain dissatisfied with the outcome of their complaint to the school, a complaint can be made to the Information Commissioner's Office who will then investigate the complaint and take action where necessary.

11 Security and Confidentiality

All staff and governors must ensure that information relating to identifiable individuals is kept secure and confidential at all times. The school will ensure that its holdings of personal data are properly secured from loss or corruption and that no unauthorised disclosures of personal data are made.

The school will ensure that information is not transferred to countries outside the European Economic Area (EEA) unless that country has an adequate level of protection for security and confidentiality of information which has been confirmed by the Information Commissioner.

12 Rights of Data Subjects

Individuals wishing to request their information as a subject access request should contact the school, who will arrange for the information to be processed in accordance with the Data Protection Act. Further information on this is available in a separate document, *How to access your records.*

Individuals should also make requests in writing to the school if they wish to exercise their other rights under the legislation.

APPENDIX 1

DATA PROTECTION PRINCIPLES

First Principle

processed lawfully, fairly and in a transparent manner in relation to individuals;

Second Principle

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

Third Principle

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

Fourth Principle

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

Fifth Principle

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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

Sixth Principle

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.