St Osburg's Catholic Primary School

GDPR
Data Protection Policy
Approved by Governors – April 2018

1. PURPOSE

1.1 The General Data Protection Regulations 2016 and subsequent domestic legislation replace the EU Data Protection Regulation 1995 and the Data Protection Act 1998 in an aid to update and manage a technologically advancing world. In order to provide adequate protection to these changes, the EU have increased the accountability of data controllers/processors and enhanced the rights of individuals.

The School has notified the Information Commissioner's Officer of its data processing and its registration number is Z6383884

The objective of this policy is to establish a framework that ensures the School has in place structures and processes to manage the security of personal data collected, processed and stored by the School and requests to access information held by the School so as to:

a. ensure requests are dealt with in compliance with the requirements of the General Data Protection Regulations; and

b. ensure that the School employees are aware of their obligations in relation to security of personal data, recording processing activities and in providing access to information held by the School in accordance with the law.

1.2 A further objective of this policy is to provide a framework through which effective record management can be achieved.

1.3 The School's governing body retains overall responsibility for policy implementation, whereby individual staff members are required to abide by the procedures and systems put in place as a result of policy implementation and to support it. This policy will be communicated to all employees who will be expected to fulfil their responsibilities as detailed below.

1.4 This policy applies to all premises and activities within the control of the School and is supported by arrangements for implementation and monitoring.

1.5 The Data Protection Officer acts as a representative for the School with regard to its data controller responsibilities. The Data Protection Officer's details can be found on the School's Privacy Statement.

2. GENERAL PRINCIPLES OF THE GDPR

2.1 The School is a public authority and a Data Controller that is dependent upon its records collection and management systems for the discharge of its educational responsibilities. As a 'data controller' any third party suppliers that also process personal data are called 'data processors'. Under GDPR and domestic data protection legislation, data processors, alongside Data Controllers, can be held directly responsible should there be a data breach.

As a Data Controller, the School commits to ensure that:

- Personal data is processed lawfully fairly and in a transparent manner;
- Data is collected for a specified, explicit and legitimate purpose and not further processed;
- Data is adequate, relevant and limited as it must not be excessive in relation to the reason it has been collected (or processed);
- Data is updated regularly and every reasonable step is taken to ensure it is accurate;
- Individuals can request the restriction and erasure of their data and data can be rectified, removed and that can be blocked if it is incorrect;
- Data is kept in accordance with sound record retention and archiving procedures;
- Data is protected against accidental, unlawful destruction, alteration, processing and disclosure.

3. INDIVIDUAL RIGHTS

GDPR and domestic data protection legislation provides the following rights for individuals:
3.1 The right to be informed
3.2 The right to access
3.3 The right to rectification
3.4 The right to erasure
3.5 The right to restrict processing
3.6 The right to data portability
3.7 The right to object
3.8 Rights in relation to automated decision making and profiling

4. LAWFUL BASIS FOR PROCESSING

4.1 The responsibilities of the School to process information will predominantly fall under the lawful basis of Public Task; the processing is necessary for you to perform a ***task*** in the ***public*** interest.
4.2 The individual will be informed at the point of personal data collection of the lawful basis for processing.

4.3 Consent

4.3.1 In order to collect and process data that does not fall under the umbrella of the Public Task or the alternative lawful processes outlined in the GDPR and domestic data protection legislation, the School will seek to gain freely given, informed and unambiguous consent to collect information from:

a. a child with capacity unless consent specifically relates to processing information online (in which case this will be a child over the age of 13 with capacity); or
b. a parent/guardian of that child who holds parental responsibility.

4.3.2 The School recognises its responsibility to ensure that any collection of data for children without capacity is consented to by the parent(s) or carers who hold parental responsibility.
4.3.2 The School recognises that if it accepts consent from a holder of parental responsibility over a child, in order to process their personal information it will need to gain the personal consent of the child once the child has either;

a. gained a developed sense of understanding and competence; or
b. reached the age of maturity in terms of online services (13 years).

4.3.3 The School recognises that this age of competence will vary from child to child.

4.4 The Right to Erasure and to Object

4.4.1 The School ensures that pupils/parents are made aware at the time of giving consent how consent can be withdrawn. The School ensures this process is easily accessible for all individuals providing consent.
4.4.2 The School recognises that pupils, parents and staff have a right to object to their personal data being processed in relation to marketing materials and agree to the immediate termination of that processing if they receive an objection from the individual or on the verification of an individual's objection provided for on behalf of another.

5. OBLIGATIONS OF THE SCHOOL

5.1 It is committed to creating, storing and managing its records securely, efficiently accurately and effectively. The School recognises that this is necessary to support its core functions, to comply with legal requirements and for its operational and information needs and to contribute to the effective management of the institution. It also recognises that efficient, accurate, secure and effective record

management is helpful to the wider support of staff and students and contributes to the safeguarding of their health, safety and welfare.
5.2 To underpin the collection of information, processing and management of records, the School will endeavour to ensure:
a. the regulation of efficient creation, storage, maintenance and destruction of records including pseudonymisation;
b. that information will only be shared if the appropriate parents, carers or pupils have been notified of this via a privacy notice prior to the collection of the personal data or with their unequivocal consent;
c. the sharing of individuals' data will be in relation to a legal obligation, a data sharing agreement or a contractual arrangement;
d. the efficient and effective maintenance of the School academic, management and administrative systems;
e.the upkeep of staff training in regard to data protection;
f. the secure retention, retrieval and destruction of records, in compliance with statutory and School requirements;
g. regular audits are conducted to ensure the compliance of General Data Protection Regulations via the Data Protection Officer;
h. the creation and maintenance of accurate and complete records in order to maximise efficiency, adopting the 'privacy by design' approach;
i. that a record is kept of the information being processed;
j. the delivery of services to staff, students and stakeholders in a consistent and equitable manner using computerised systems, where appropriate;
j. a continuity of service in the event of a disaster.

6. ORGANISATIONAL SCOPE

6.1 This policy applies to the School and to any commercial organisations or service providers (including agencies or consultancy companies) contracted to carry out work for the School.

7. POLICY STATEMENT

7.1 In order to support its compliance, the School will adhere to the principles and codes of practice enshrined in the GDPR and domestic data protection legislation.
7.2 The School will increase openness, promote transparency and demonstrate accountability by supporting the proactive sharing of information with its parents/ carers, pupils, employees and those who come into contact with the School.
7.3 The GDPR and domestic data protection legislation gives individuals the right to know what information is held about them, how it is processed and subject to certain exemptions, receive a copy of that information. It also provides a framework to ensure that personal data is handled appropriately.

8. SUBJECT ACCESS REQUESTS

Subject Access Requests and Individuals

8.1 The School's policy is to ensure that:
a) Information is provided in a timely manner in response to Subject Access Requests, unless a statutory exemption applies;
b) The request will be recorded and monitored;

d) In response to Subject Access Requests that fall under GDPR applicants are informed whether the School holds the information requested and are provided with it. The School will respond to all Subject Access Requests within 30 calendar days of receipt of a valid request in the format it was requested, unless an exemption is applicable, the request is onerous, the request is vexatious, the information is publicly available or the subject has previously made an identical request and it was completed satisfactorily. Any such refusal will be approved by the Senior Leadership Team and the named Data Protection Officer;
e) Complaints regarding how a Subject Access Request has been dealt with are managed through an Appeal Procedure'. Any such appeal must be promptly directed to the Data Protection Officer as required by the Procedure;
f) The Senior Leadership Team is responsible for co-ordinating requests for information under the GDPR and domestic data protection legislation and issuing responses;
g) Personal Data is not disclosed to third parties except where disclosures are permitted by, or are required by, law or under an obligation of contract;
h) The School will maintain and publish information through the School's website, which commits the School to make certain information readily available, and explain how the public may access it.

Subject Access Requests and Staff Members

8.2 In the event of a Subject Access Request, staff may be asked to provide all details, hard copy or electronic, concerning personal information of that individual to the Senior Leadership Team.
8.3 Where a non-work (i.e. private) email account is used to conduct work-related communications and/or official School business and the School reasonably suspects that information concerning the School's official business is held on that private account, The School shall require that individual to search their private email account. A record of the action taken will be recorded by the School. School Personnel should note that they may be guilty of a criminal offence if they altar, deface, block, erase, destroy or conceal any record held by or on behalf of School, with the intention of preventing the disclosure of all, or any part, of the information that the applicant would be entitled to under GDPR and domestic data protection legislation. The discovery or suspicion of any such offence must be reported immediately to management and the named Data Protection Officer and may be referred to the police. This policy applies to all recorded information held by the School in any format, including text message, messages sent over instant messaging networks, Facebook messages and other forms of electronic communications where they relate to the business of the School, whether sent using official or private accounts.
8.4 Personal Data will, under normal circumstances, only be disclosed to a third party after written consent from the individual concerned has been obtained or the disclosure falls under an alternative legal basis, alongside a privacy notice being brought to the individual's attention.
8.5 However, the requirement to obtain consent may be overridden in the event that the data falls within: a) an information sharing protocol or contract; b) one or more of the exemptions under the GDPR and domestic data protection legislation; or c) a court order or Parliamentary statute.
8.6 To ensure that where relevant and / or where appropriate a Fair Collection Notice (FCN) or Privacy Notice will, where necessary, be displayed at the head of forms, requiring the disclosure of personal data from an individual. The School's standard privacy statement can be found on its website**.** This notice will inform the individual completing the form why their information is being collected, with whom it will be shared and why, what will be done with it, where it will be stored and for how long.
8.7 In exceptional circumstances, staff will take reasonable action to inform the responsible authorities or employers of relevant Personal Data where there is a risk from others, a risk to an

individual or where School receives lawful authority to disclose personal information or where there is an emergency situation based on the lawful basis of vital interests.

9. RECTIFICATION OF INFORMATION

9.1 Staff will regularly liaise with pupils and parents to ensure an adequate process of updating information.
9.2 However, staff will also allow parents/pupils to update their details through the normal means of contact with the School.

10. DATA RETENTION

10.1 The School will effectively implement a record retention schedule.

11. DATA IMPACT ASSESSMENTS

11.1 Information Risk is considered and afforded a priority in decisions within School in the same way as financial and operational risk. The School agrees to conduct Data Impact Assessments whenever a new process is implemented that presents a significant risk to pupil, parent or employee personal data and/or where a new digital system is implemented. The School recognises that as a Data Controller, the decision to carry out a Data Impact Assessment lies with it. However, the implementation of a Data Impact Assessments will be conducted with the guidance of the School's Data Protection Officer.
11.2 Data Impact Assessments will be recorded in a format recommended by the Information Commissioner's Office and stored in a safe and secure system where risk assessments are usually placed, accessible to authorised individuals only.
11.3 Information risk will be managed by a process of identifying, controlling, minimising and/or eliminating risks that may affect School's information or information systems.

12. DATA SECURITY

12.1 The School recognises its obligations to safely store documents that hold personally identifiable information.
12.1.1 **Non-Electronic Files**:

a. Storage of hard copies will be kept in locked cabinets, secure desk drawers and individual rooms will have access cards/key locks to allow authorised entry only.
b. In the event that hard copy documents containing personal information need to be physically transported, they will be stored in a secure wallet with an authorised individual.

12.1.2 **Electronic Files**:

a. Electronic Files will be stored on a database that is password protected and allows only authorised staff member access.
b. In the event that files containing personal information need to be sent, moved or shared, they will be encrypted and password protected to ensure they are available to authorised individuals only.
c. Where necessary, pseudonymisation of files will be implemented.

12. RESPONSIBILITY FOR ACCESS TO INFORMATION

12.1 Overall responsibility for disclosure of Personal Data lies with the Senior Leadership Team.
12.2 The Governing body will endeavour to ensure effective implementation of this policy and put in place mechanisms for its review in line with guidance from the School's named Data Protection Officer.

12.3 Each individual employee is responsible for actively supporting this policy. School personnel are responsible for promptly retrieving information where they are requested to do so for the purpose of responding to a subject access request.
12.4 School employees must seek advice in the event of uncertainty in relation to this policy.
12.5 Senior Leadership Team in conjunction with the named Data Protection Officer's guidance, are responsible for ensuring that School Personnel within their area of control are aware of this policy and are adequately trained in the handling of information and Subject Access Requests.
12.6 School Personnel must familiarise themselves with their obligations via the rolling programme of staff training, specifically, procedures and guidance available.
12.7 The Data Protection Officer has responsibility for the following tasks:
a) To oversee the development and review of this Data Protection Policy, Privacy Notice, Record Retention Policy and relating documents.
b) The interpretation of this policy, for monitoring compliance with the policy and for providing advice and guidance on its implementation.
c) To develop procedures and guidance to enable staff to carry out their own effective record management, ensuring that procedures are published and communicated to Senior Leadership Team and trickled down.
d) To act as a competent person regarding data protection, by providing guidance for subject access requests and record management.
e) To ensure that Subject Access Requests are dealt with efficiently and effectively, meeting legislative requirements.
f) To provide advice and guidance to staff on security of information, access to information and record management.
g) To identify current and proposed legislation relevant to School and inform School management.
k) Be responsible for liaising with the Information Commissioner's Office on any matter relating to School's handling or resolution of a Subject Access Request, incident or breach of the GDPR or domestic data protection legislation.

13. ICO CONTACT

13.1 If an individual (staff member, parent or student) believes that their data has been compromised they can send a complaint to the 'Data Controller' who will forward this on to the Data Protection Officer for guidance or they can send a complaint directly to the ICO:

Information Commissioner's Office
Wycliffe House,
Water Ln,
Wilmslow
SK9 5AF
Telephone: 0303 123 1113, Monday-Friday 9am-5pm.

Appendix

Definitions

GDPR: General Data Protection Regulation 2016 and all legislation operating within England enacted in relation to these Regulations.

Personal Data: means any information relating to an identifiable natural person, whether they can be directly or indirectly identified by reference to name, identification number, online identifier, or to specific things such as physical, physiological, genetic, mental, economic, cultural or social identity factors. You will often see this in reference to the term Natural Person.

Special Category Data: As above but this is called Special Category personal data and needs to be looked after very carefully; it refers to very specific groups of personal data such as race or ethnic origin, political views, trade union membership, genetic and biometric data, health and sexual orientation. It should not be collected unless it is necessary.

ICO: The Information Commissions Office is the UKs Supervisory Authority, which is the organisation that oversees data protection in England, Wales and Northern Ireland and, to a limited extent, in Scotland. The Commissioner is the regulator appointed by the Crown to promote public access to official information and protect personal information.

Information and processing: any information, data or records, irrespective of format or medium, which are generated or processed. Examples include electronic communications, e-mails, video recordings, hardcopy (paper) files, images, graphics, maps, plans, technical drawings, programs, software and all other types of data. Processing is a collective term when you collect, use, share or store data. The GDPR focuses specifically, but not completely, on digital data such as used in computers, phones and tablets, and on websites.

Data Controller: is the person or organisation that an individual has allowed, or is obliged, to hold their personal details on the lawful basis of Public Interest. The Data Controller decides what, why, how, where and when personal data is processed. A School is most often the Data Controller.

Domestic Data Protection Legislation: The Data Protection Act 2018 [subject to royal assent] and any other applicable domestic data protection legislation.

Data Processor: This is a person or organisation that the Data Controller has asked to 'do something' with the data they control. They must only 'do' what is allowed in the data sharing agreement. They are breaking the law if they use this data for any other purpose. In a number of cases, the Data Controller and the Data Processor is the same person or organisation. If a School collects and uses the data, without it being shared or processed with anyone else, then they are both Data Controller and Data Processor. Data Controllers need to have a Data Sharing Agreement in place with Processors to outline agreed processing and confidentiality obligations.

Subject Access Request (SAR): request made by, or on behalf of, a data subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

Privacy notice: This is your notice to the world about the way you handle information you have access to. Every School must have one already and it's important that all staff know what it says and means. It should also be in clear language so it can be easily understood by parents and children, where relevant.

Lawful basis for processing: Also referred to as legal basis for processing. No organisation can process data unless there is a legal reason for doing so. There are six main categories for lawful processing; consent, contract, legitimate interests, vital interests, public task, legal obligation. The majority of the School's ability to collect and process personal data will rely on the lawful basis of

'Public Task' or 'Legal Obligation'. It may on occasion rely on consent, although this can easily be withdrawn.

Encrypted Data: This is when the data is scrambled and only a key (such as a password) can align the data to make it identifiable. Personal data that leaves a safe and secure environment must be encrypted.

Data Breach: This is a breach of security, a breach of availability or data that is not correct when it should be; where accidentally or unlawfully personal data has been destroyed or misused. This might lead to physical or mental harm to an individual.

Data Impact Assessment (DIA): Is a tool used to identify and reduce the privacy risks. It is particularly used when implementing new systems. A DIA is written evidence that you have been through this thought process. The School uses Risk Assessments for safeguarding and H&S and a DIA should be an automatic response when sharing data with a new source.

Privacy by Design: This means you consider data protection and privacy from every angle. It is beneficial to internalise this method prior to implementing a procedure/process.

Data Erasure/Right to be forgotten: An individual can ask the Data Controller to remove and stop processing their personal data. If the Data Controller can justify it needs to process this data, then the request can be refused.

Data Protection Officer (Data Protection Officer): An expert on data protection who works independently to oversee that data protection policies and issues are correctly managed. See 1.5 for details.

Pseudonymisation: This is a process that is used a lot in education where data is analysed and presented in reports or for examples, but the links to identify individuals are removed.