Holy Rosary Catholic Primary School

Data Protection Policy
Incorporating the provisions of the General Data Protection Regulation (GDPR)

This policy applies to Holy Rosary Catholic Primary School and is drawn up in compliance with the General Data Protection Regulation and Data Protection Act 2018 following advice and guidance published by the Information Commissioner's Office (ICO).

Definitions and explanations

The Information Commissioner's Office (ICO)
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO has powers to fine bodies who are in breach of their obligations under the legislation. Holy Rosary is required to register with the ICO and our registration number is: **ZA346089** . Full details of our registration can be viewed at https://ico.org.uk/ESDWebPages/Entry/**ZA346089**.

The General Data Protection Regulation (GDPR) and the Data Protection Act
This is a European Directive which will become part of UK law in May 2018 in the Data Protection Act 2018 (which replaces the Data Protection Act 1998). The Data Protection Act 2018 (DPA) will remain in force after Brexit. For more details see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The aim of the GDPR
The GDPR and the DPA exist to protect the data of individuals. They contain a series of safeguards for every individual built around the principles of privacy, confidentiality, respect and security. The GDPR is a response to the need to protect individual rights in an increasingly digital world.

Scope of the GDPR
It applies to everyone, including businesses, schools, academies and academy trusts. Holy Rosary is classed as a Public Body and as such has more obligations placed upon it than other organisations. Holy Rosary has a mandatory obligation under the DPA to comply with the provisions of the GDPR.

What is classed as data under the GDPR and DPA?
Any information that relates to a living person that identifies them – their **Personal Data**. This can include, name, address, phone number, IP address, National Insurance Number for example.
Some data is considered to be more sensitive – an individual's **Sensitive Data.** This can include data relating to racial or ethinic origin, details about that person's opinions, political affiliation, religious or philosophical beliefs, trade union membership, health, sexual

orientation, genetic or biometric data, Special Educational Needs and medical information for example, where any of these are processed in a way which could identify an individual.

What Data does Holy Rosary Collect?
We collect and use personal and sensitive data about staff and pupils, and will hold personal data about parents and other individuals who come into contact with us. This information is gathered in order to enable us to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that we comply with our statutory obligations.

Privacy by Design and Privacy Impact Assessments
The requirement that privacy must be designed into the processing of personal data by default has always been a principle for data protection. It has now been brought to the fore in the new legislation. Organisations with technologies and processes that are likely to result in a high risk to the rights of the data subjects are required to carry out a Privacy Impact Assessment.

Data Subject
Someone whose details we keep on file (paper or electronic, in a formal file or elsewhere).

Data Controller
The body who has overall responsibility for how the organisation manages data. The Data Controller will delegate the day to day management of this to data processors on its behalf. Holy Rosary Governing Body is the Data Controller.

Data Processor
This is the person or organisation that collects, uses, processes, accesses, amends and shares the data that the Data Controller has collected or has authorised to be collected. It can be a school, an academy, a member of staff, a third party company, a governor, a contractor or a temporary employee. It can also be another organisation such as the police or the Local Authority.

Data Protection Officer
The person appointed by the Data Controller to advise the Data Controller about its statutory obligations under the GDPR and DPA, to monitor compliance against those obligations, to provide advice about the data protection impact assessment, to be the point of contact for Data Subjects, to manage breach procedures, to advise on training. The Data Protection Officer for Holy Rosary is:
John Walker: john@jawalker.co.uk

Data Protection Policy

1. The Principles
This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the DPA and GDPR, and other related legislation. It will apply to data regardless of the way it is collected, used, recorded, stored and destroyed, and

irrespective of whether it is held in paper files or electronically. All staff at Holy Rosary will be made aware of the importance of safeguarding data and those involved with the collection, processing, sharing and disclosure of personal and sensitive data will receive specific training so that they can carry out their duties and responsibilities in compliance with the guidelines in this policy. Holy Rosary will adopt the principle of Privacy by Design in all its activities and will comply with the six principles of GDPR.

i. ***Personal data shall be processed lawfully, fairly and in a transparent manner:*** We must have a legitimate reason to hold the data. We explain this in the Privacy Notices published on our website and attached at Appendix 1a and 1b. Where we need to we will ask for consent to use or share data for a particular purpose. If you wish to withdraw consent then we have a form for you to complete to allow us to process your request. This is published on our website and attached at Appendix 2. There are situations when you cannot withdraw consent and these are explained in Data Subject Rights at 2. below.

ii. ***Personal data shall be obtained only for one or more specified and lawful purposes:*** This means that we must not use data for any other purposes other than those originally given and that we must state the purpose when we collect the data. 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 and is allowable.

iii. ***Personal data shall be adequate, relevant and not excessive:*** We will collect the minimum amount of data needed for a particular task or reason. This ensures that in the unlikely event of there being a breach or a hack then only limited data can be lost.

iv. ***Personal data shall be accurate and where necessary, rectified and kept up to date:*** We collect data when pupils join us and we will keep this up to date annually. If an individual feels that the information held is inaccurate, should no longer be held or should not have been held originally then a request should be made in writing to the Data Protection Officer who will investigate and confirm the action that has been taken.

v. ***Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose:*** We have a Records Retention Policy and schedule which is published on our website and data will be stored in line with that schedule.

vi. ***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:*** We have processes in place to keep data safe. This

includes paper files and electronic records. Our Information Security Procedures are attached at Appendix 3.

2. Data Subjects' Rights

Individuals have a right:

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, ie to limit what is done with their data
- to object to data being shared or collected
-

There may be occasions when Data Subjects are also themselves the subject of child protection and safeguarding concerns and we may share their data for the prevention and detection of crime. We will have a duty to share data in these circumstances in addition to sharing information with organisations such as the Department for Education, the Catholic Education Service, Social Care, the Local Authority, and HMRC, amongst others. In some cases these obligations override data subject rights.

3. Subject Access Request

You can ask for copies of information that we hold about you or a pupil who you have parental responsibility for. This is referred to as a Subject Access Request and we have provided a form and guidance on how you should do this at Appendix 4.

4. Processing Data

We must have a legitimate reason to collect and process data about an individual and must process it lawfully. We will collect and process data with regard to the following conditions:

i. ***The legal basis*** and authority we rely on for collecting and processing data are:
   - consent has been gained from the data subject or their parent
   - performance of a contract where the data subject is a party
   - compliance with our legal obligations
   - to protect the vital interests of the data subject or other associated person
   - to carry out the processing that is in the public interest and/or official authority
   - it is necessary for the legitimate interests of the Data Controller or third party
   - in according with national law

ii. In addition any special (sensitive) categories of personal data will be processed on the grounds of:
   - explicit consent has been granted from the data subject or their parent
   - it is necessary to comply with employment rights or obligations

- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate interests of Holy Rosary
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- Child Protection and Safeguarding
- national laws relating to the processing of genetic, biometric or health data

iii. ***Data sharing*** will only be done within the limits set by the GDPR. We are obliged to follow guidance and instructions from the Nottingham Roman Catholic Education Service, the Catholic Education Service, Department for Education, the Education, Skills and Funding Agency, Companies House (if we are an academy), the NHS, the Police, the Local Authority and other specialist organisations and will share information where it is required to do so. The basis for sharing or not sharing data are recorded.

iv. ***Breaches and Non Compliance*** will be handled in accordance with the procedures set out in Appendix 5. We expect that breaches will be rare as protecting and maintaining data subjects' rights is the purpose of this policy. However we will be open and transparent in identifying and reporting breaches to the relevant authorities and data subjects.

v. ***Consent*****:** We will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required. However in most cases data will only be processed if explicit consent has been obtained. Consent is defined by the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmation action, signifies agreement to the processing of personal data relating to him or her". We may seek consent from young people also, and this will be dependent on the child's age and capacity and the reason for processing.

On the website we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

On joining us as a member of staff or pupil you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other relevant purposes, as set out on the Data Collection Consent form.

Obtaining clear consent and ensuring that the consent remains in place is important for us. We also want to ensure the accuracy of the information that

we collect so we check the accuracy of the data we hold by asking you to update the Data Collection and Consent form annually to let us know whether your details or your decision about consent changes.

vi. ***Withdrawing Consent***: Consent can be withdrawn subject to contractual, statutory or regulatory constaints, Where more than one person has the ability to provide or withdraw consent we will consider each situation on its merits and within the principles of GDPR and also child welfare, protection and safeguarding principles. We have provided a form for you to withdraw consent and this is at Appendix 2.

vii. ***Physical Security***: For every secure area we have individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, ie locked. Offices and cupboards that contain personal data will be secured if the processor is not present. The Business Manager/Premises Manager/ICT Manager/ is responsible for authorising access to secure areas under the instruction of the Headteacher. All staff, contractors and third parties who have access to lockable areas must take due care to prevent data breaches.

viii. ***Electronic Security***: We take appropriate measures to ensure that electronic data is password protected, encrypted and that permissions are granted only in so far as they are necessary to perform the task and no more. The School will ensure that *"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against the accidental loss or destruction of, or damage to, personal data."*

5. Secure Disposal of Data

Whenever data is destroyed or disposed of we will ensure that this is carried out in compliance with the GDPR. Documents will be held in the secure archive pending destruction which will be in line with the retention schedule. Paper copies will be disposed of using an approved and compliant contractor. The destruction of electronic data will be overseen by the ICT Manager or Business Manager using approved and compliant organisations.

The destruction of memory sticks, hard drives, PCs, laptops and other electronic devices will be under the direction of the ICT Manager or Business Manager.

6. Third Parties

A WRITTEN AGREEMENT WILL BE IN PLACE BETWEEN THE THIRD PARTY DATA PROCESSOR AND OURSELVES TO CONFIRM COMPLIANCE WITH THE GDPR PRINCIPLES AND OBLIGATIONS TO ASSIST US IN THE EVENT OF A DATA BREACH OR SUBJECT ACCESS REQUEST, OR ENQUIRIES FROM THE ICO.

7. CCTV

We do not currently operate CCTV. However if we do install CCTV we will register its use with the ICO and will develop a CCTV policy.

8. Training for staff, governors and directors

All existing staff will be trained under the new guidelines. All staff will be required to sign to say that they understand the principles of GDPR and their role in protecting data. New staff will be required to undertake training as part of induction. Refresher training will be provided annually. Our Codes of Conduct and Disciplinary Policies will be updated to include specific references to everyone's responsibilities under the GDPR. Existing governors and directors will be trained on their role as Data Controllers and Data Processors under the new guidelines. New governors and directors will receive training as part of induction.

9. Complaints

If you have a concern about how your data has been collected, used, held or processed then please refer to the Complaints Procedure in the first instance which is available on our website. You have a right to complain if you feel that data has been shared without consent or lawful authority, or if you have asked us to erase, rectify, not process data and we have not agreed to your request. We will always seek to resolve issues on an informal basis, and then through our formal complaints procedure. If you have not been able to resolve your complaint informally then please complete the form contained in the Complaints Policy and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for enforcing the DPA obligations and their contact details can be found at www.ico.org.uk Helpline: 0303 123 1113 Email: casework@ico.org.uk

10. Policy Review

A review of the effectiveness of our GDPR compliance and processes will be conducted by the Data Protection Officer every 12 – 24 months and reported to the Governing Body.

The Data Protection Officer for the School is:
John Walker: john@jawalker.co.uk