



***GENERAL DATA PROTECTION REGULATION
POLICY
OUR LADY & ST JOSEPH CATHOLIC PRIMARY
SCHOOL***

PREPARED BY: P Devereux

APPROVED BY: Governing Body

DATE: July 2018

REVIEW DATE: July 2020

CHECKED DPO: May 2018

This document is a statement of the aims and principles of the school, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Our Lady & St Joseph Primary School needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Our Lady & St Joseph School must comply with the General Data Protection Regulation 2018.

In summary these state that personal data shall be:

- Processed fairly, lawfully, and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Held for no longer than necessary
- Processed in a manner that ensures appropriate security of the personal data

Our Lady & St Joseph School and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the school has developed this General Data Protection Regulation Policy.

Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the school from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller/Designated Controller and The Data Protection Officer

The school as a body corporate is the Data Controller, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controller and Data Protection Officer will deal with day to day matters.

Designated Data Controller: Mr Patrick Devereux

Data Protection Officer: Mrs Lucy Henderson/Louise Manthorpe

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or their child should raise the matter with the Data Protection Officer.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the school in connection with their employment is accurate and up to date.

- Informing the school of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The school cannot be held responsible for any errors unless the staff member has informed the school of such changes.

If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the Schools GDPR Policy.

Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- Information or data about pupils is shared with other staff as appropriate using the secure email provider.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, safe or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer or safe.

Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the school holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the school is doing to comply with its obligations under the General Data Protection Regulation

This Policy documents addresses in particular the last three points above. To address the first point, the school will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the school holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have right under the General Data Protection Regulation to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing to the Data Protection Officer

The school aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days, of the request as required by the General Data Protection Regulation.

Subject Consent

In many cases, the school can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, as defined in the General Data Protection Regulation, express consent must be obtained. Agreement to the school processing some specified classes of personal data is a condition of acceptance of employment for staff. This included information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The school has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job.

The school has a duty of care to all staff and students and must therefore make sure that employees and those who use school facilities do not pose a threat or danger to other users.

The school may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The school will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the school is a safe place for everyone, or to operate other school policies, such as the Sick Pay Policy or the Equalities Policy.

Because this information is considered sensitive under the General Data Protection Regulation, staff (and pupils where appropriate) will be asked to give their express consent for the school to process this data. An offer of employment may be withdrawn if an individual refuse to consent to this without good reason.

Publication of School Information

Certain items of information relating to school staff will be made available via searchable directories on the public web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the school.

Retention of Data

The school has a duty to retain some staff and student personal data for a period of time following their departure from the school, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

Disposal of confidential data

Any documents containing confidential data will be disposed of carefully, either in confidential shredding bins or other secure shredding facilities

ICT equipment

Where scrap ICT equipment consists of processors, hard drives, disks etc. which contain data covered by the General Data Protection Regulation or information of a confidential nature, the equipment must be disposed of via the Local Authority facility or a Local Authority approved facility and the appropriate charges paid.

Missing assets

The Headteacher should cause enquiries to be made as to the whereabouts of the missing items. A report should be made to the Finance and Resources Committee. Where crime is suspected the police should be informed. If the item is insured a claim should be instigate

Conclusion

Compliance with the General Data Protection Regulation is the responsibility of all members of the School.

Any deliberate breach of the General Data Protection Regulation Policy may lead to disciplinary action being taken, or even to a criminal prosecution.