Vigo Primary School

GDPR Policy

This policy has been approved and adopted by the Governing Body in March 2022 and will be reviewed in March 2025

The school collects and uses personal information (referred to in the General Data Protection Regulation (GDPR) as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The school is the Data Controller, of the personal data that it collects and receives for these purposes.

The school has a Data Protection Officer (Mike Christmas), who may be contacted at Vigo Primary School.

The school issues Privacy Notices (also known as a Fair Processing Notices) to all pupils/parents, governors and staff. These summarise the personal information held about pupils, governors and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data

Purpose

This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information/ data?

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles

The GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes)
3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. Personal data shall be processed in a manner that ensures appropriate security of the personal

In addition the are six lawful basis for processing personal data These are:
(a) **Consent**: the individual provides clear consent to process their personal data for a specific purpose (as defined by the school);
(b) **Contract**: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose, for example, staff employment contract or pupil placement;
(c) **Legal obligation**: the processing is necessary for the School to comply with the law (not including contractual obligations);
(d) **Vital interests**: the processing is necessary to protect someone's life;
(e) **Public task**: the processing is necessary for the School to perform a task in the public interest/official functions, and the task or function has a clear basis in law;
(f) **Legitimate interests**: the processing is necessary for a legitimate interest or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests.

The School will generally rely on the following three legal bases for processing data as follows:
(a) Consent;
(b) Contract;
(c) Legal obligation.

Duties

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

Commitment

The school is committed to maintaining the principles and duties in the GDPR at all times. Therefore the school will:

- Inform individuals of the identity and contact details of the data controller
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the EEA the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information
- Inform individuals of their data subject rights
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests)
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
- Ensure that all staff and governors are aware of and understand these policies and procedures.

Data Breaches

Definition: A data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure or access to personal data.

Reporting obligations: Any actual data breach or alleged data breach must be reported to the Data Protection Officer as soon as it is discovered, whatever time that might be, to enable its circumstances to be investigated and appropriate action taken to limit any damage and to prevent a similar occurrence. As soon as the School becomes aware of a significant data breach as determined by the Data Protection Officer it has 72 hours in which to report the breach to the Information Commissioner's Office.

Examples of breaches and their seriousness for reporting purposes are:

- mistakenly sending an email or letter containing personal data to an incorrect recipient.
- theft of IT equipment containing personal data.
- failing to deal with a Subject Access Request.

If a breach is found to be sufficiently serious i.e. if not dealt with it is likely to result in a high risk to the rights and freedoms of individuals e.g. resulting in discrimination, damage to reputation, financial loss – through identity theft or otherwise – loss of confidentiality or any other significant economic or social disadvantage then not only does this breach have to be reported to the ICO within 72 hours of its discovery, the individuals concerned must be notified of the breach in a timely manner as directed by the Data Protection Officer.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years. The policy review will be undertaken by the Data Protection Officer, Head teacher and governing body.

Contacts

If you have any enquires in relation to this policy, please contact Mrs Sarah Smith who will also act as the contact point for any