Old Vicarage School

Data Protection Policy

Old Vicarage School collects and uses personal information about staff, pupils, parents, governors and other individuals who come into contact with the School. 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 the School complies with its statutory obligations.

The purpose of this policy is to ensure that the personal information we collect is handled in compliance with legal requirements and secured against unauthorised access. It applies to all information 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 are required to read and understand this policy to ensure they are aware of their duties and responsibilities in relation to the protection of this data and the consequences of failure to comply.

Personal Information

Personal information is defined as data which relates to a living individual who can be identified from that data.

The School Privacy Notice explains how and why we collect personal information and what we do with that information. It also explains the rights individuals have in relation to their personal information. A copy of this Notice is provided to all parents and members of staff. It is also available on the School public website ('Policies' page) and on the Staff Server ('Policies' folder) on the School Network.

Responsibilities

The School's Compliance Officer, Alison Povall, is responsible for data protection compliance within the School. If you have any questions or comments about the content of this policy, or if you need further information, please contact her.

Data Protection Principles

The School is required to comply with enforceable data protection principles when collecting and processing personal information.

We do this by ensuring that:

- We collect personal information for specified and legitimate purposes only.
- We process personal information lawfully, fairly and in a transparent manner.
- The personal information we process is adequate, relevant and necessary.
- We take reasonable steps to ensure that the personal information we hold is kept accurate and up to date.
- We do not keep personal information for longer than is necessary.
- We take appropriate measures to keep personal data secure.

Information Security – Storage and Access to Data

The School ensures that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which is recorded.

Physical controls

- Appropriate building security measures are in place, such as alarms, swipe card/code access, CCTV and deadlocks. The computer server room is kept locked.
- Visitors to the school are required to sign and an out, wear identification badges whilst in the school and are, where appropriate, accompanied.
- Hard copies of personal information are securely stored out of sight.
- Secure waste bins and shredders are installed for secure disposal/destruction of paper copies.

Technical measures

- The School database system is set up so that users are assigned a clearance that determines which files are accessible to them.
- Access to protected data files on the School network is controlled according to the role of the user.
- Access to the School network and externally hosted IT systems are password protected. Staff are required to change their network passwords on a regular basis.
- The School has clear procedures for the automatic backing up, accessing and restoring of all data held on school systems.

Use of external organisations

- The School uses external organisations to help process personal information on its behalf. Our contracts with those organisations contain specific clauses to safeguard the security of this information.

Cloud Based Storage

- Personal information may be stored on servers outside the UK but within the European Economic Area (EEA).
- The School is aware that personal data held in remote and cloud storage must be protected in line with the Data Protection Act and will ensure that it is satisfied with the protection controls put in place by the data services providers.

Data Protection Impact Assessments (DPIA)

- When considering any new plans to process personal data, the School will undertake a DPIA to assess if the data processing is necessary and proportionate in relation to its purpose, and what measures can be taken to protect the information.

Staff Training and Guidelines

Staff are provided with data protection training that is appropriate for their role. All members of staff are required to follow the guidelines below to reduce the risk of personal data being compromised. Staff should ensure they:

- Only access the personal information that they have authority to access, and only for authorised purposes.
- Do not provide personal information to individuals who are not members of staff, unless they have specific authority to do so.
- Take particular care with the security of special (sensitive) personal information such as medical records (physical & mental), criminal records (DBS checks), and any data relating to religion, race/ethnicity, sexuality, political affiliations and trade union memberships.

- Do not send photos of pupils or staff for publication by external sources unless they have specific authority to do so.
- Try to avoid taking paper copies of data or personal information off the school site. If there is no way to avoid this, the information should not be left on view in public places and locked away when left unattended.
- Either shred unwanted paper copies of personal information or place them into the secure waste bins - they will be removed and shredded by a secure waste contractor.
- Take care to remove all printouts from printer trays or photocopiers.
- Lock the screens of computers and other devices when leaving them unattended.
- Use an encrypted/password protected USB stick if it is necessary to transport data offsite.
- Do not store School data (including photographs) on a home computer or personal devices.
- Use the School email for all School email communications.

Staff who are found to be in breach of any of these guidelines may be subject to disciplinary procedures.

Retention of data

Personal information should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the information was obtained. The School's Records Retention Policy sets out the relevant retention period. Where there is any uncertainty, staff should consult the Head.

Destruction of data

Personal information that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

Data Breaches

On occasion, personal data may be lost, stolen or compromised. This is called a 'data breach' and may involve both electronic media and/or paper records. It can also mean inappropriate or unauthorised access to information.

If a member of staff becomes aware that a data breach has occurred, or may occur, it must be reported it to the Head as soon as possible. Failure to comply with this obligation could result in disciplinary action being taken.

Depending on the risk to people's rights and freedoms (the impact on the affected individuals), the School may be required to report the data breach to the Information Commissioner's Office (ICO) within 72 hours. Penalties for data protection breaches include monetary penalties, enforcement and audits.

Signed: **Gill Linthwaite**
Head

Date of review: May 2020
Date of next review: May 2022