Jon Pritchard

GENERAL DATA PROTECTION AND PRIVACY POLICY

1 Company Aims

The Company aims to ensure that all personal data collected about staff, suppliers, contractors, customers, volunteers other individuals is collected, stored and processed in accordance with the **General Data Protection Regulation (GDPR)** and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. Also, the Company will comply with the Payment Card Industry Data Security Standard (PCI DSS). This is a set of security standards designed to ensure that ALL companies that accept process, store or transmit credit card information maintain a secure environment. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2 Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests**.**

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3 Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number

	• Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, health, qualifications, training or payroll details.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Religious or philosophical beliefs • Health • Sexual orientation and gender • Disability • Nationality
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person who processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4 The Data Controller

The Company processes personal data relating to staff, suppliers, contractors, customers, volunteers' other individuals and therefore is a **Data Controller**.

5 Roles and Responsibilities

This policy applies to all staff employed by our Company**,** and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

6 Directors

The Directors have overall responsibility for ensuring that our Company complies with all relevant data protection obligations.

7 All staff

7.1 Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Company of any changes to their personal data, such as a change of address
- Contacting the Company in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals

- If they need help with any contracts or sharing personal data with third parties

8 Data Protection Principles

The GDPR is based on data protection principles that our Company must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

9 Retention of Data

Where personal data is held in paper or other manual form, the default period for retaining data has expired and none of the exceptions for retaining data beyond the default period is satisfied, the Company will ensure the data is shredded or otherwise confidentially disposed of.

Where data is held in an electronic format the Company will where feasible use its reasonable endeavours to:

- Put the data beyond use so that the data is no longer on a live electronic system and cannot be accessed other than the Data Controller
- Ensure individuals within the Company do not and will not attempt to access the data or use the data in any way
- Surround the data with such technical and security measures to ensure it is not accessible
- Permanently delete the data from the Company electronic systems when and where this becomes possible

10 Collecting Personal Data

10.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Company can fulfil a contract with the individual, or the individual has asked the Company to take specific steps before entering into a contract.
- The data needs to be processed so that the Company can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.
- The data needs to be processed so that the Company can perform a task in the public interest and carry out its official functions.
- The data needs to be processed for the legitimate interests of the Company or a third party (provided the individual's rights and freedoms are not over-ridden)
- The individual has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

10.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

11 Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with an individual that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff or customers for example IT, Accountancy and Payroll companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

12 Data Protection Rights of the Individual

Individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Company**.** If staff receives such a request, they must immediately forward it to the relevant Manager**.**

13 CCTV

We use CCTV in various locations around Company sites. We will adhere to the ICO's code of practice for the use of CCTV. We are allowed camera surveillance in the work place. The purpose is to reduce the risk of theft and damage to exhibits.

The Company believes the cameras are not intrusive and there is still some privacy elsewhere on our premises. Individuals have the right to see any footage in which they feature and individuals can make a request by writing. Details of storage and retention periods are also available.

Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to a relevant Manager.

14 BACS and Selling Activities

As a Company, we may collect additional Personal Data from you in relation to BACS payments and selling activities.

Information you provide to us: In some cases, if you pay us by BACS, we will collect financial information from you (e.g. your bank account information or an address to send cheques) as necessary to facilitate payments and information required for tax purposes.

Information we obtain from other sources: We may also collect or receive Personal Data from third party sources, such as third-party websites, your bank and credit reporting agencies.

When placing an order, customers will have the opportunity to advise and confirm if they wish to receive any future marketing or other information from us. Under the GDPR above, without this confirmation we cannot send any such information, unless we have a pre-existing business relationship. In that case customers can advise if they do not want to continue to receive information from us. We must stop all marketing communication at that point

We will retain contact, order and our invoicing details on our system for all transactions. However, individuals have the **'right to be forgotten'** and anyone wishing to be removed from our records can request this and we will delete contact information from our records within 30 days of receiving the request, unless we need to retain them for legitimate reasons. However, details of any transactions will be retained for the statutory time to comply with VAT and Taxation regulation.

To ensure we maintain the level of security described above: -

- All our internet activities are fully protected behind a firewall configuration to keep customer personnel data secure.

- All activities are protected by internally created passwords which are regularly monitored and changed.

- We store BACS details in a Google Drive file storage system on our fully secure encrypted web server. All customer activities and details relating to payment are undertaken through and maintained by our bank.

- Each Data Processor has an individual username and password to allow them to access internet banking and only authorised personnel, including those from third party supplies are able to access sensitive parts of the system, including data records and physical access to Servers and PC's.

- Our systems are regularly scanned to ensure we are not holding any unauthorised payment details.

- We have virus, malware and phishing protection software in place and these are updated automatically as soon as new editions or updates to existing are released.

- All staff are aware of the above policy and are actively engaged in ensuring implementation.

15 Customer and Supplier Data

Staff will not reveal anything about:

- Customer details we hold on record
- Suppliers details, transactions, pricing etc.
- Information about our business or systems or equipment

16 Data Protection

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified Data Controller and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.
- Completing privacy impact assessments where processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.

- Maintaining records of our processing activities.

17 Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or

- Papers containing confidential personal data must not be left on office and vehicles desks, on staff desks, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information in non-electronic format needs to be taken off site, staff must sign it in and out from the Offices.
- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff who store personal information on their personal devices are expected to follow the same security procedures as for Company-owned equipment**.**
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

18 Personal Data Breaches

The Company will make all reasonable endeavours to ensure that there are no personal data breaches. When appropriate, we will report the data breach to the ICO within 72 hours.

19 Training

All staff are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

20 Monitoring Arrangements

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every 2 years.