PEL PRIVACY AND DATA POLICY – MAY 2018

0.1 INTRODUCTION

Partnership Education Ltd (PEL) is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations. We hold personal data about our employees, clients, suppliers in order to fulfil our contractual obligations and to function as a Business providing ICT Support and Consultancy services. This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work.

0.2 DEFINITIONS

Personal Data - 'Personal Data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data may include: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

Special categories of personal data - Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information — any use of special categories of personal data should be strictly controlled in accordance with this policy.

Data Controller - 'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

Data Processor - 'Processor' means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

Processing - 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

0.3 SUPERVISORY AUTHORITY

This is the national body responsible for data protection. The supervisory authority for our organisation is [the Information Commissioners Office].

0.4 THE PRINCIPLES

PEL shall comply with the principles of data protection ("the Principles") enumerated in the EU General Data Protection Regulation ("GDPR"). We will make every effort possible in everything we do to comply with these principles.

The Principles are:

1. **Lawful, fair and transparent -** Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.
2. **Limited for its purpose -** Data can only be collected for a specific purpose.
3. **Data minimisation -** Any data collected must be necessary and not excessive for its purpose.
4. **Accurate -** The data we hold must be accurate and kept up to date.
5. **Retention -** We cannot store data longer than necessary.
6. **Integrity and confidentiality -** The data we hold must be kept safe and secure

1 DATA POLICY

1.1 LAWFUL BASIS FOR SHARING DATA

PEL holds data in order to be able to carry out the activities detailed in contractual agreements with clients.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Where PEL requires data in order to fulfil a contract
- Marketing our business
- Improving services

1.2 DATA WE HOLD ABOUT CUSTOMERS

Contact information for billing and contracts. - This may include Name, Email, Phone Number, Job Title

IT Assets – Information on the IT estate in order to agree and understand the scope of equipment supported under contract. Includes Make, model, Serial Number, location on Site, Date of Purchase

Licencing – Records held of licence entitlement in order to remain compliant while providing support services.

Marketing Information – Where consent is granted, records of individuals indicating an interest in procuring services from PEL are stored.

Site ICT Documentation – Information held in order for staff to carry out maintenance tasks on Customer systems under an active contract. Includes System Logins, Machine names, Software Configuration, Log files.

1.3 SPECIAL CATEGORIES OF PERSONAL DATA

What are special categories of personal data?

Previously known as sensitive personal data, this refers to data about an individual which is more sensitive, so requires more protection. This includes data such as that relating to race, ethnic origin, or any other sensitive information about an individual. PEL does not hold this type of information for any Client data, and does not foresee a requirement to do so in future.

Storage of data relating to Pupil / Students

PEL does not hold any information relating to pupil / student data on internal systems or devices. Data relating to pupil/students remains on the systems owned or registered to the client.

2 RETENTION OF RECORDS

Records detailing contracts and are kept in line with standard retention periods in order to comply with legal and financial compliance.

Contact information stored for the purposes of providing services are obtained at the beginning of each contract and regularly reviewed, and can be amended at any time by request. We will only hold contact details for as long as we require to in order to comply with contractual obligations or due to the fact that it is in our legitimate interest to do so.

Marketing information is only stored where consent is given, and where PEL believes there is an active interest in services offered. Unsubscribe options will be made available within any communications, and records can be amended or removed upon request at any time.

2.1 END OF RELATIONSHIP

At the point of contract termination, PEL will destroy copies held in relation to network documentation, passwords, and remove any software tools providing monitoring or remote access.

3 PROTECTION OF RECORDS

- PEL IT systems are based in the registered UK offices and a secure UK datacentre.
- All staff are issued company laptops and phones, which are locked down in line with internal policies, with patch management, Anti-Virus, and configuration management agents.
- Data stored on devices is minimised, with VPN configuration allowing access back to datacentre shared areas.
- Where remote access tools are used to access Customer systems, these are used with two factor Authentication and strong password policies.
- Log files record access to endpoints with the software installed.
- Passwords are stored using Password management software. Two Factor authentication is required to access the store, and user accounts providing access are managed centrally.

3.1 HOW WE DEAL WITH SUBJECT ACCESS REQUESTS

PEL will provide an individual with a copy of their personal information if requested. This will be supplied within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats.
If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting.

4 RESPONSIBILITIES WHERE PEL IS CONTRACTED AS A DATA PROCESSOR

Customers contracting PEL remain the Data Controller for the data belonging to/ and produced by the customer. PEL will act as a Data Controller and abide by the below principles to ensure it supports the customer in their responsibility as Data Controller.

As a Data Processor, we must only act on the documented instructions of a Data Controller. We acknowledge our responsibilities as a Data Processor under GDPR and we will protect and respect the rights of Data Subjects.

- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations
- Nothing will be done by either the controller or processor to infringe on GDPR

4.1 INHERITED POLICIES

Where PEL is under contract to support a customer's systems, PEL will adopt a customer's local policy in relation to data, and report to the local DPO or responsible staff member.

PEL will act under the instruction of the local DPO or responsible staff member in relation to:

- Retention, creation, and storage of data.
- Backups of data
- New starter / leaver process
- Password policy
- Access rights
- Disposal of equipment

4.2 STAFF TRAINING AND AWARENESS

PEL staff are trained in the core principles of data management and GDPR. All staff working with customer data are required to complete this training, and it is included in the staff induction process. These are certified courses, which all PEL employees must complete as part of their compliance training.

Staff access to sensitive data will occur in the nature of providing information when requested by school staff, configuring access to, and testing access to data. Staff will not disclose, share or duplicate data, and will report to the Schools DPO or responsible person on any issues they identify where data is being misused by school staff.

4.3 SAFEGUARDING

PEL has a defined Safeguarding Policy available from the website or on request. All staff are aware of the importance of Safeguarding and Child protection, and complete Safeguarding training.

4.4 STORAGE OF DATA

School data accessed by PEL staff in accordance with their duties under contract to provide ICT support is only processed in the location defined by the customer. Data is not duplicated to portable devices, attached to emails, or removed from site, unless under the instruction of the sites DPO or nominated person for specified purposes.

4.5 CUSTOMER EQUIPMENT REMOVED FROM SITE

Removing customer equipment for repair is avoided if possible, with repairs conducted on the customer site. On occasions where it is agreed to be necessary to remove school owned equipment, it will be stored in secure workshop facility. Where the equipment contains data, and is deemed beyond economical to repair, this will be returned to site to be processed by the customers approved WEEE registered carrier.

4.6 HOSTED PLATFORMS

PEL does not currently provide hosted services where customer data would reside on storage owned or leased by PEL. Many sites do now use Google G-Suite and Microsoft 365. Hosted systems remain registered to the Customer, and their use governed by the Customers Data policies.

Both Microsoft 365 and Google G-Suite have extensive policies around Data protection and are GDPR Compliant. Further information available currently at:

Microsoft GDRP Resources: https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/FAQ

Google GDPR: https://cloud.google.com/security/gdpr/

4.7 3RD PARTY SUPPLIERS AND TOOLS

PEL undertake a rigorous process of reviewing 3rd Party Suppliers and sub-contractors prior to undertaking any activity with them. Suppliers are reviewed as part of the Supplier review processes in maintaining the ISO 9001:2015 accreditation.

Supplier review processes include enhanced analysis of a supplier's data policy and commitment to GDPR. Any supplier that does not satisfactorily demonstrate a commitment to data and privacy protection will not be considered as a partner of PEL.

4.8 CONTACT

If you wish to contact us to make a Subject Access Request, request rectification or object, please contact our Privacy Manager via email to companysecretarial@ptsconsulting.com.