Data Protection Policy

Introduction

Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our staff, and we recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, clients, contractors and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to legal safeguards specified in the Data Protection Act 2018, incorporating General Data Protection Regulation EU 2016/679, and other regulations (collectively known as the "the Data Protection Requirements") impose restrictions on how we may use that information.

This policy applies to all individuals working at any level within the company including: employees (whether permanent, fixed-term or temporary); subcontractors, sub-consultants seconded staff and agency staff; or any other person associated with us, wherever located (collectively referred to as staff or employee in this policy).

Status of the Policy

This Policy sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, recording, editing, revising, use, storage, transfer and destruction, and other processing of personal information.

This policy does not form part of any employee's contract of employment and it may be amended at any time.

All individuals are responsible for acting in accordance with the requirements of the Data Protection Policy. Compliance with this Policy is mandatory. The People, Quality and Development (PQD) team oversee the implementation and review Data Protection Policy. The Directors of TEP take ultimate responsibility for data protection.

If you have any concerns or wish to exercise any of your rights under this policy, then you can contact PQD on 01925 844004 or inbox@pqd.uk.com

Definition of data protection terms

Data is information which is stored electronically, on a computer, on premises server, in the cloud, or in certain paper-based filing systems.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

Data protection principles

TEP complies with the data principles set out below. Anyone processing personal data must comply with the seven enforceable principles of good practice ensuring that all data is:

- Processed fairly, lawfully and in a transparent manner;
- Collected and processed for limited purposes and in an appropriate way;
- Adequate, relevant and not excessive for the purpose;
- Accurate, and where necessary, kept up to date;
- Not kept longer than necessary for the purpose;
- Secure; and

  Accountable

Fair and lawful processing

The Data Protection Requirements are intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual. Individuals must be told who the data controller is (in this case TEP), who the data controller's representatives are (in this case the Directors), the purpose for which the data is to be processed by TEP, and the identities of anyone to whom the data may be disclosed or transferred.

In accordance with the Data Protection Requirements we will only process personal data where it is required for a lawful purpose. Lawful purposes include (amongst others): where the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business.

Sensitive Personal Data

Some of the information we hold about staff is sensitive and we are aware that special rules apply to it. We will not collect and use such data unless the individual has given us explicit consent (for example, confirmed in writing that they agree to us holding it) or we need it in order to fulfil our obligations as an employer. Where it is considered necessary to collect data within explicit consent this will only be sanctioned by the Head of PQD to ensure compliance with the Data Protection Policy.

Processing for limited purposes

Personal data is only be processed for the specific purposes notified to the individual when the data was first collected or for any other purposes specifically permitted by the Data Protection Requirements. Personal data will not be collected for one purpose and then used

for another. If it becomes necessary to change the purpose for which the data is processed, the individual will be informed of the new purpose before any processing occurs.

Adequate, relevant and non-excessive processing

Personal data will only be collected to the extent that it is required for the specific purpose notified to the individual. Any data which is not necessary for that purpose will not be collected in the first place.

Accurate data

Personal data is reviewed for accuracy and kept up to date. PQD ensure the accuracy of personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data is destroyed.

Timely processing

Personal data will not be kept longer than is necessary for the purpose. Data will be destroyed or erased from our systems when it is no longer required.

Processing in line with data subject's rights

We process and observe all personal data in line with individuals' rights under the Data Protection Requirements, in particular their right to:

- Confirmation as to whether or not personal data concerning an individual is being processed;
- Request access to any data held about them (see also Subject Access Requests below);
- Request a rectification, erasure or restriction on processing of their personal data;
- Lodge a complaint with a supervisory authority;
- Data portability - where data has been stored amongst the physical and virtual estate;
- Object to processing including for direct marketing; and
- Not be subject to automated decision making

All data stored within the TEP domain is located within recognised software systems including MS Access and SQL server limiting any issues with data portability.

Data security

We ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

TEP has procedures and technologies to maintain the security of all personal data from the point of determination of the means for processing and point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it;
- I**ntegrity** means that personal data should be accurate and suitable for the purpose for which it is processed; and
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs (other than Directors).

Security procedures include the following which are applicable to both office and home working:

- **Entry controls**: Any stranger seen in entry-controlled areas within TEP offices should be reported;
- **Secure lockable desks and cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential) and TEP's Clear Desk Policy implemented;
- **Secure Server Room:** with coded lock restricted to designated ICT Team members;
- **User Access Control:** to provide access to restricted files and folders;
- **Methods of disposal:** Paper documents should be shredded. Computer hardware data storage should be physically destroyed when they are no longer required and appropriate WEEE certificates provided;
- **Equipment:** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- **Locations:** all sensitive data is controlled through secure access based on the domain controller restrictions on user accounts; and
- **Home-working Security Measures:** the above measures shall also apply to home-working settings.

To ensure security, you must not disclose personal data – in writing or verbally – to anyone not authorised to receive it, whether internal or external, within or outside the workplace.

Data Breaches

What is a Data Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This can include a breach either through accident or through a deliberate action.

A personal data breach can include:

- The loss, destruction, corruption or disclosure of personal data
- Access or release of personal data without the correct authorisation

- Malicious encryption of personal data or accidental destruction or loss
- Access of personal data by an unauthorised third party
- Sending of personal data to an incorrect recipient
- Theft or loss a computer devices containing personal data
- Alteration of personal data without permission

Under the Data Protection Regulations it is clear that once a data breach has occurred an agreed set of actions must be followed. These actions have been considered taking into account the risk posed people, the likelihood and severity of any risk to people's freedoms.

Individuals must immediately notify their team manager, ICT and PQD of any breaches of security which lead or could lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will allow us to:

- Investigate the failure and take remedial steps if necessary;
- Consider the risk posed by the data breach; and
- Make any applicable notification within the mandatory legal timescales.

PQD will lead a review and identify if TEP is required under the Data Protection Regulations to report any breach of security involving personal data to the data protection regulator, the Information Commissioners Office (ICO) or equivalent. Advice will be sought from the ICO if required. If reported to the ICO the following information will be provided as minimum:

- Description of the data breach;
- Date and time of breach if known;
- Timeline of actions and resources;
- Details on the numbers of people affected;
- Action Plan;
- Lead Contact.

Dealing with subject access requests

TEP has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to.

A formal request from an individual for information that we hold about them must be made in writing. Employees wishing to make a request can use the Personal Data Subject Access Request form (annexed to this policy). Any member of staff who receives a written request should forward it to PQD immediately.

All requests will be considered without undue delay and within one month of receipt as far as possible.

Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it;
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked;
- Refer to their line manager for assistance in difficult situations.

Authorised Data Locations

Any personnel information or data can only be securely stored within the agreed, restricted and authorised data locations. Access to authorised data locations is restricted to only those staff members with specific responsibilities for the management of personal data. The list below details the authorised data locations. Staff must not have any personnel information or data stored anywhere outside of these authorised locations.

TEP Databases:

- Contacts Database
- Health and Safety Database
- Subconsultant Database

SharePoint2013

- People Details
- Personnel
- Recruitment
- Business Continuity

Server Infrastructure

- TEP SQL01
- TEP SQL02
- TEP SQL03

Finance / HR Software

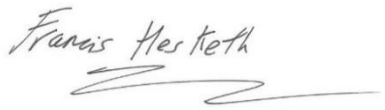
- Opera
- Sage Payroll
- Sage HR

Consequences of Failing to Comply

TEP takes compliance with this policy very seriously. Failure to comply puts both staff and the Company at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, up to and include dismissal, in line with TEP's Discipline and Grievance Policy.

Individuals may apply to the courts for compensation if they have suffered damage from such a loss. TEP may incur fines if we are in breach of the Data Protection Requirements, and employees may also be personally liable for fines or imprisonment if they steal, or recklessly misuse personal data.

Date of Next Review: January 2024



Person with overall responsibility	Francis Hesketh, Director

Rev	Date	Description of Amendment	Authorised by
00	October 2011	Original Issue	Cath Neve
01	07 March 2013	Update footer and change font to Arial	Cath Neve
02	May 2015	Updated to provide correct contact for Subject Access Requests. Amended to include Sub-consultants and Sub-Contractors.	Cath Neve
03	June 2015	Update header & footer	Graeme Atherton
04	March 2016	Added signature box	Hayley Chriscoli
05	January 2017	Updated to include improved security measures	Francis Hesketh
06	June 2018	Updated to comply with GDPR EU 2016/279	Katie Shilcock
07	January 2019	Scheduled review, no amendments	Katie Shilcock
08	October 2021	Updated to include security measures for home-working. Also added form for General Subject Access Requests and updated to reflect new TEP branding	Katie Shilcock