

1. Background Policy Statement

- 1.1 TPT Consultancy & Training regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between it and its employees, board members, employment applicants, former employees, Customers (defined below), consultants, contractors, suppliers and partners.
- 1.2 TPT Consultancy & Training recognises that individuals have a right to privacy and fully endorses and adheres to the principles of data protection as set out in the Data Protection Act 1998 ("DPA").
- 1.3 In addition, TPT Consultancy & Training's employees and board members are required to treat information which is available to them concerning TPT Consultancy & Training or its Customers, consultants, contractors, suppliers, partners, employees, board members, employment applicants and former employees in the strictest confidence.

2. Purpose and Scope

- 2.1 This policy aims to protect and promote the rights of individuals and TPT Consultancy & Training. It identifies information that is personal data and also information which is to be treated as confidential. It gives general guidelines for processing such information (defined below).
- 2.2 The policy covers all records and information held by TPT Consultancy & Training which contain personal data and/or confidential information held in relation to employees, board members, employment applicants, and former employees, Customers, consultants, contractors, suppliers and partners.

Author:	Tom Townsend	Approved by:	Tom Townsend
Revision Level:	01	Date of Issue:	June 11

3. Definitions

3.1 TPT Consultancy & Training

3.1.1 TPT Consultancy & Training is a training provider to companies within the Aerospace, Defence, Rail and Automotive Sectors.

3.2 Customers

3.2.1 Persons/Companies to whom TPT Consultancy & Training provides training

3.3 Personal Data

3.3.1 Data relating to a living individual who can be identified from that data (or from that data and other information in possession of TPT Consultancy & Training). Personal data can be factual, e.g. name, address, date of birth, or it can be an opinion, e.g. performance appraisal. Such information normally has the individual as its focus and affects their privacy in some way.

3.3.2 Personal data may be held on paper forming part of a relevant filing system or on a computer or other electronic media.

3.4 Processing

3.4.1 Any activity that involves use of the 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.

3.4.2 The processing of personal data must comply with the eight data protection principles under the DPA. These provide that personal data must be:

- Processed fairly and lawfully
- Processed for limited purposes and in an appropriate way
- Adequate, relevant and not excessive for the purpose
- Accurate
- Not kept longer than necessary for the purpose
- Processed in line with data subjects' rights
- Secure.
- Not transferred to people or organisations situated in countries without adequate protection.

3.5 Sensitive Personal Data

3.5.1 This includes information about a person's racial or ethnic origin, their political opinions, religious or similar beliefs, physical or mental health, sexual life or proceedings for any offence.

Author:	Tom Townsend	Approved by:	Tom Townsend
Revision Level:	01	Date of Issue:	June 11

3.6 Confidential Information

3.6.1 This comprises all commercially sensitive data, whether received formally, informally, or discovered by accident. This includes, but is not necessarily limited to:

- Any personal data about employees, associates, employment applicants, Customers, consultants, contractors, suppliers and partners;
- Any policy, procedure or strategy deemed by the Board or Senior Management Team to be commercially sensitive;
- Any other information, not in the public domain, that is likely to be commercially sensitive or where there is risk of TPT Consultancy & Training being damaged by its disclosure;
- Tenders and quotations for services

4. Responsibilities

4.1 It is the responsibility of employees and board members to process personal data correctly and maintain confidentiality as set out in their contracts of employment/service agreements and within this policy. The inappropriate disclosure of information may be treated as a disciplinary offence including, where appropriate, gross misconduct and dealt with accordingly.

4.2 It is the responsibility of all employees to inform a senior manager when they are made aware of a breach of confidentiality. The senior manager is responsible for taking appropriate action when made aware of a breach of confidentiality.

4.3 Processing of information - the 8 data protection principles

1. Fair and lawful processing

Processing of data must be done fairly and without adversely affecting the rights of the data subject. The data subject should be told who the data controller is (in this case, TPT Consultancy & Training), the purpose for which the data is to be processed and the identities of anyone to whom the data may be disclosed or transferred.

The individual must consent to the processing or the processing must be necessary for a legitimate interest. When processing Sensitive Personal Data, additional conditions must be met. In most cases the individual's explicit consent to the processing of such data is required.

Author:	Tom Townsend	Approved by:	Tom Townsend
Revision Level:	01	Date of Issue:	June 11

2. Processing for limited purposes

Personal data may only be processed for the specific purposes notified to the individual or for any other purpose permitted by the DPA. Personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose, the individual must be informed of the new purpose before any processing occurs.

We will not attempt to gain access to information that is not necessary for them to hold.

3. Adequate, relevant and non-excessive processing

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject.

4. Accurate data

Personal data must be accurate and kept up to date. Steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

5. Timely processing

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from TPT Consultancy & Training's systems when it is no longer required.

6. Processing in line with data subject's rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them (see Subject Access Requests below).
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Author:	Tom Townsend	Approved by:	Tom Townsend
Revision Level:	01	Date of Issue:	June 11

7. Data security

TPT Consultancy & Training must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

TPT Consultancy & Training is required to put in place procedures and technologies to maintain the security of all personal data. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, as follows:

- **Confidentiality** - only people who are authorised to use the data can access it. Employees handling confidential information must ensure that this information remains confidential.
- **Integrity** - personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** - authorised users should be able to access the data if they need it for authorised purposes. Personal data should be stored on TPT Consultancy & Training's central computer system instead of individual PCs.

Security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported immediately.
- **Methods of disposal.** Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required

8. Transfer to other countries

Data must not be transferred to people or organisations situated in countries without adequate protection.

Author:	Tom Townsend	Approved by:	Tom Townsend
Revision Level:	01	Date of Issue:	June 11

5. Confidentiality Guidelines - Working in the Office

- 5.1 Adopt a culture of ensuring anonymity by using a code such as the resident's account number (or applicant's reference number) when producing reports for the public domain;
- 5.2 Be aware of who else may be listening, particularly in areas open to the public, i.e. talking to residents in reception;
- 5.3 At the end of the day get into a routine of clearing away all confidential information from your desk; locking desks and filing cabinets;
- 5.4 Never leave confidential documents unattended: place the documents in an envelope and place in your drawer;
- 5.5 Always "lock" your PC when you are away from your desk. Please refer to the IT/Security Policy for further information.

6. Confidentiality Guidelines - Working away from the Office

- 6.1 Employees must obtain advance authorisation from their line manager to take work away from the office;
- 6.2 Once authorisation is granted, identify which pieces of work will be taken away from the office. Managers should encourage employees to limit the material they take away from the office;
- 6.3 Only in exceptional circumstances should the whole file be taken away from the office;
- 6.4 Ensure that your documents cannot be observed if you read or process documents on public transport;
- 6.5 Do not leave documents or laptops in unattended vehicles;
- 6.6 Store documents safely out of view at home and do not show them to other household members.

Author:	Tom Townsend	Approved by:	Tom Townsend
Revision Level:	01	Date of Issue:	June 11

7. Confidentiality Guidelines - General Conduct

7.1 The disciplinary rules draw attention to issues of confidentiality. Therefore the following guidelines apply:

- Do not discuss or disclose confidential information outside the office with interested third parties, or with family and friends, who have no particular right to know about the internal business of TPT Consultancy & Training;
- Do not discuss confidential information internally. Be aware that we all have a responsibility only to discuss those matters of business that we are privy to within our own sections/departments and with other members of staff only where they have a legitimate right to know;
- Do not leave confidential information on voicemails or e-mails;
- Do not gain, or attempt to gain, access to information which you are not authorised to have;
- Sensitive Personal Data should not be transmitted via e-mail unless adequately encrypted, or in a password protected attachment.

8. Handling of Personal Data and Confidential Information

8.1 Personal data and confidential information relating to Customers, consultants, contractors, suppliers and partners is held on the housing database, the main file server, the e-mail system and files in the relevant operational departments.

8.2 Information relating to applications made by prospective employees will usually be held for a period of time not exceeding twelve months from the date of the closing date set out in the advertisement. After this period, the application forms of candidates not selected for employment will be destroyed. Anonymous information may be retained, including equal opportunities statistics of candidates for each position advertised.

8.3 Information relating to customers will be held as long as necessary to perform TPT Consultancy & Training's functions.

8.4 Employment application forms will contain a paragraph outlining how the application form will be used and seeking "consent" from the applicant. Customers will be given a form outlining the data processing expectations and seeking consent from the individual.

Author:	Tom Townsend	Approved by:	Tom Townsend
Revision Level:	01	Date of Issue:	June 11

9. Disclosure of Information

9.1 Personal data and confidential information held will only be passed to other organisations on a need-to-know basis and with an individual's consent unless there are exceptional circumstances. Exceptional circumstances include:

- where there is clear evidence of fraud;
- to comply with the law;
- in connection with legal proceedings;
- where it would be essential to enable TPT Consultancy & Training to carry out its duties e.g. where the health and safety of an individual would be at risk by not disclosing the information or where there is a legal requirement to do so;
- Anonymously for statistical or research purposes

9.2 Personal data may only be transferred to a third-party data processor if the third party agrees to comply with appropriate security procedures and policies.

10. GENERAL

10.1 Personal data - Subject Access Requests

10.1.1 Associates and Customers may make a request for personal data which TPT Consultancy & Training holds about them. Such request must be made in writing and should be submitted to TPT Consultancy & Training's Data Controller.

10.2 Training

10.3 All employees responsible for handling personal data and confidential employee information will receive training on this policy and it will be included as part of the induction programme for new staff who are required to handle such information.

10.4 Monitor and Review

10.5 Files will be monitored on an on-going basis to ensure that they comply with this policy.

10.6 This policy and its procedure will be reviewed every two years to ensure that it is effective and complies with current good practice. A review will be carried out sooner should there be any changes to statutory requirements.

Author:	Tom Townsend	Approved by:	Tom Townsend
Revision Level:	01	Date of Issue:	June 11