



1. General principles

- 1.1 PTS recognises that colleagues (employees, volunteers, students, apprentices, associates, and others who work within our organisation) gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential, and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential or not.
2. This policy aims to give guidance but if in doubt, seek advice from your line manager.
 - 2.1 Information received by PTS as part of the services it provides, will be considered to be information for PTS to share with colleagues within the organisation and use to deliver its aims and objectives.
 - 2.2 Colleagues should inform groups, organisations, or individuals why they are requesting information and explain the purpose of storing and using this information. Colleagues should ask permission to keep and use this information.
 - 2.3 Colleagues are able to share information with their Line Manager in order to discuss issues and seek advice. Colleagues will not disclose to anyone, other than their line manager, any information considered sensitive, personal, financial, or private without the knowledge or consent of the individual, or an officer, in the case of an organisation.
 - 2.4 Colleagues should avoid exchanging personal information or comments (gossip) about individuals with whom they have a professional relationship.
 - 2.5 Colleagues should avoid talking about organisations or individuals in social settings.
 - 2.6 There may be circumstance where colleagues would want to discuss difficult situations with each other to gain a wider perspective on how to approach a problem.
 - 2.7 If colleagues receive information from individuals outside PTS regarding the conduct of a colleague or group, then this should be dealt with sensitively. The appropriate colleague should tell the individual about the Complaint Procedure and advise them accordingly.
 - 2.8 If employees are dissatisfied with the conduct of a colleague and have sensitive information that could be evidenced through investigation, they should discuss it with the appropriate line manager under the Whistle Blowing Procedure. Any allegation, which is found to be malicious, or ill-founded, will be dealt with by PTS under the Disciplinary Procedure.
 - 2.9 Where there is a legal duty on PTS to disclose information, the person affected will be informed that disclosure has or will be made.

3. Why information is held.

- 3.1 Most information held by PTS relates to individuals, employees, and associates.
- 3.2 Information is kept enabling PTS to understand the needs of individuals in order to deliver the most appropriate services.
- 3.3 Information about users may be kept for the purposes of monitoring our equal opportunities policy and also for reporting back to funders.

4. Access to information

- 4.1 Information is confidential to PTS as an organisation and may be passed to colleagues and line managers.
- 4.2 Where information is sensitive, it will be confidential to the employee dealing with the case and their line manager. Such information should be clearly labelled 'Confidential'

and should state the names of the colleagues entitled to access the information and the name of the individual or group who may request access to the information.

- 4.3 Colleagues will not withhold information from their line manager unless it is purely personal to them and not business related.
- 4.4 Candidates and users may see PTS records which relate to them or their organisation. The request must be in writing to the Managing Partner giving 14 days' notice. The letter must be signed by the individual, or in the case of an organisation's records, by the Chair or Executive Officer or Manager.
- 4.5 Sensitive information as outlined in point 3.2 will only be made available to the person or organisation named on the file.
- 4.6 Employees may see all of their personnel records by giving 14 days' notice in writing to the Managing Partner.
- 4.7 When photocopying or working on confidential documents, colleagues must ensure they are not seen by people in passing. This also applies to information on computer screens.

5. Storing information

- 5.1 General non-confidential information about organisations is kept in unlocked filing cabinets that are available to PTS colleagues.
- 5.2 Information about other individuals will be kept in filing cabinets by the colleague directly responsible. Colleagues must ensure line managers know how to gain access.
- 5.3 Employees' personnel information will be kept in lockable filing cabinets by line managers and will be accessible to the Managing Partner.
- 5.4 Files or filing cabinet drawers bearing confidential information should be labelled 'confidential'.
- 5.5 In an emergency situation, the Managing Partner may authorise access to files by other people.
- 5.6 Ensure confidential documentation or personal data is shredded before putting in the recycling bins.

6. Duty to disclose information.

- 6.1 PTS has a legal duty to disclose some information including:
- 6.2 Reporting of Safeguarding issues that involve children or vulnerable adults. (This will follow the process in the PTS safeguarding policy.)
- 6.3 Drug trafficking, money laundering, acts of terrorism or treason will be disclosed to the police.
- 6.4 In addition, colleagues believing an illegal act has taken place, or that a user is at risk of harming themselves or others, must report this to the Managing Partner who will report it to the appropriate authorities.
- 6.5 PTS should inform the users of this disclosure.

7. Disclosures

- 7.1 PTS complies fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and
- 7.2 Disclosure information.
- 7.3 PTS will request pre-employment Disclosure and Barring Service (DBS) checks for new employees involved in contact with vulnerable adults, as specified by the Disclosure Guidance.
- 7.4 PTS will clearly state the need for, and level of, Disclosure on the recruitment advert.
- 7.5 PTS will keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, and the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

8. Data Protection Act

- 8.1 Information about individuals, whether on computer or on paper, falls within the scope of the Data Protection Act and must comply with the data protection principles.
- 8.2 These are that personal data must be:
 - 8.2.1 Obtained and processed fairly and lawfully held only for specified purposes.
 - 8.2.2 Adequate, relevant and not excessive
 - 8.2.3 Accurate and up to date
 - 8.2.4 Not kept longer than necessary
- 8.3 Processed in accordance with the Act: -
 - 8.3.1 Kept secure and protected.
 - 8.3.2 Not transferred out of Europe
 - 8.3.3 PTS will ensure that it complies with all aspects of the Data Protection Act. Please refer to PTS Data Protection Policy for detailed information on how we will do this.

9. Breach of confidentiality

- 9.1 Colleagues who are dissatisfied with the conduct or actions of other colleagues or PTS should raise this with their line manager using the grievance procedure, if necessary, and not discuss their dissatisfaction outside PTS.
- 9.2 Colleagues accessing unauthorised files or breaching confidentiality may face disciplinary action. Ex-employees breaching confidentiality may face legal action.