Paperless World Limited

Security Policy Statement

Contents

Section 1: Paperless World Limited Security Policy Statement

Paperless World Limited ("PWL") is committed to a policy of protecting the rights and privacy of individuals [including staff and individuals it has dealings with] in accordance with the principles of the Data Protection Act 1998.

PWL, in the conduct of its business, needs to process certain information about individuals for administrative purposes e.g. recruitment, payment of staff, administration of programmes, to collect fees and for purposes of complying with the legal obligations to funding bodies and government. In accordance with the law, information about individuals collected must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff of PWL. Any breach of the Data Protection Act 1998 is considered an offence and in that event, PWL disciplinary procedures will apply. Individuals working or have dealings with PWL with access to personal information will be expected to have read and comply with this policy.

Section 2: The Data Protection Act 1998

The Data Protection Act 1998 widen the scope of the Data Protection Act 1984 with the purpose of protecting the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and wherever possible, is processed with their consent.

Section 3: Definitions

Personal Data:

Data relating to a living individual who can be identified from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller. This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive Data:

Refers to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and offences and alleged offences. Sensitive data is subject to stricter conditions of processing.

Data Controller:

A person (either alone or jointly or in common with other persons e.g. an organisation) who determines the purposes for which and the manner in which any personal data is, or is to be, processed.

Data Subject:

Any living individual whose personal data is held by an organisation.

Processing:
Any operation relating to obtaining, recording or holding the data. This includes organisation, adaptation or alteration, retrieval, consultation, disclosure, dissemination, otherwise making available, and the alignment, combination, blocking, erasure or destruction of the data.

Third Party:
Any individual/organisation other than the data subject, the data controller [PWL] or its agents.

Relevant Filing System:
Paper or other manual filing system structured so that information about an individual is readily accessible. As defined by the Act, personal data can be held in any format, electronic [websites and e-mails], paper based, photographic etc. from which the individual's information can be readily accessed.

Section 4: Responsibilities under the Data Protection Act
PWL as a body corporate is the data controller as defined by the Act

Compliance with data protection legislation is the responsibility of all members of PWL who process personal information.

All staff of PWL is responsible for ensuring that any personal data supplied to PWL is accurate and up-to-date.

Section 5: Notification
Notification is the responsibility of the Director(s).

Section 6: Data Protection Principles
All processing of personal data must be done in accordance with the Eight Data Protection principles:

1. **Personal data shall be processed fairly and lawfully.** Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.
2. **Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.** Data obtained for specified purposes must not be used for a different purpose.
3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.** Data which is not necessary for the purpose for which it is obtained, should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted, erased or destroyed.

4. **Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.** Data must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. It is the responsibility of the individuals to ensure that data held by PWL is accurate. Individuals should notify PWL of any changes to enable data to be updated accordingly. It is the responsibility of PWL to ensure that any notification is noted and acted upon.
5. **Personal data shall not be kept longer than necessary for the purpose it was obtained.**
   Data no longer necessary for the purpose obtained must be deleted, erased or destroyed.
6. **Personal Data shall be processed in accordance with the rights of data subjects under the Data Protection Act.** [See Data Subject Rights Section 7]
7. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.** [See Section 9 on Security of Data]
8. **Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.** Data must not be transferred outside of the European Economic Area ("EEA"), the twenty five EU Member States together with Iceland, Liechtenstein and Norway, without the explicit consent of the individual. PWL should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

Section 7: Data Subject Rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision making process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Commissioner to assess whether any provision of the Act has been contravened.

Section 8: Consent

Where possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. PWL understands 'consent' to mean that the data subject has been informed of the intended processing and has signed their agreement, freely of their own accord.

Section 9: Security of Data

All staff is responsible for ensuring personal data is kept securely and that it is not disclosed to any unauthorised third party.

Personal data should be:

- kept in a lockable room with controlled access
- or in a locked drawer or filing cabinet
- if kept on the computer, password protected, or
- kept on disks which are themselves kept securely

Appropriate security measures must be in place to prevent access by unauthorised personnel by the use of confidential passwords.

Appropriate security measures must be in place for the deletion or disposal of personal data by means of shredding for manual records and disposed as 'confidential waste'. Hard drives of redundant PCs should be wiped clean before disposal.

Particular care should be taken when processing personal data "off site" at home or other locations outside PWL offices.

Section 10: Rights of Access to Data

Individuals have the right to access any personal data which are held by PWL in electronic format and manual records which form part of the relevant filing system. This includes the right to inspect confidential personal references received by PWL about that person. Any individual who wishes to exercise this right should apply in writing to the Director(s). PWL reserves the right to charge a fee for data subject access requests. Any requests will be complied with within 40 days of receipt of written request, and where appropriate, the fee.

Section 11: Disclosure of Data

PWL must ensure that personal data is not disclosed to unauthorised third parties. All staff should exercise caution when asked to disclose personal data held on another individual to a third party: in regards to an enquiry for a colleagues' work details, it would be deemed appropriate to disclose such details where that colleague is responsible for a particular function. It would, however be inappropriate to disclose a colleague's work details to someone who wished to contact them for a non-work related matter.

Best practice would be to take the contact details of the person making the enquiry and pass them to the member of PWL concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions applies:

1. The individual has given their consent (e.g. an assistant/member of staff has consented to PWL corresponding with a named third party);
2. Where the disclosure is in the legitimate interests of the organisation (e.g. disclosure to staff, personal information can be disclosed to other PWL employees if it is clear that those members of staff require the information to enable them to perform their jobs);
3. Where the organisation is legally obliged to disclose the data (e.g. HESA returns, ethnic minority and disability monitoring);
4. Where disclosure of data is required for the performance of a contract.

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- To safeguard national security *
- Prevention or detection of crime including the apprehension or prosecution of offenders *
- Assessment or collection of tax duty *
- Discharge of regulatory functions (includes health, safety and welfare of persons at work) *
- To prevent serious harm to a third party
- To protect the vital interests of the individual, this refers to life and death situations.

* Requests must be supported by appropriate paperwork.

When members of staff receive enquiries as to whether a named individual is a member of PWL, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of

PWL may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

Section 12: Retention and Disposal of Data

PWL discourages the retention of personal data for longer than it is required. A considerable amount of data is collected on current staff, volunteers, agents, temporary and casual workers. However, once a member of staff or volunteer has left the organisation, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

Staff
In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by PWL for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc will be retained for the statutory time period (between 3 and 6 years).

Information relating to unsuccessful applicants in connection with recruitment to a post will be kept for 5 years from the interview date. Personnel may keep a record of names of individuals that have applied for, be short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment/recruitment process.

Disposal of Records
Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

Section 13: Advertising, Marketing & Public Relations
Personal Data to be used for advertising, marketing and public relations purposes must inform the data subjects of this intention at the time of data collection. Individuals must have the opportunity to object to the use of their data for the above purposes (e.g. an opt-out clause on a form).

Apart from these exceptions; the Data Protection Act applies in full. The obligations to obtain consent before using data, to collect any necessary and accurate data, and to hold data securely and confidentially must be complied with.

Section 14: Further Information
PWL IT system comes under the security umbrella of ICO, for more information please visit:

Information Commissioner Office: www.ico.gov.uk