

October 2010

PEOPLE AND WORK UNIT

Data Protection Policy

GENERAL STATEMENT

The PWU is registered under the Data Protection Act 1998, meets its legal obligations under the Act and processes all personal data in accordance with the requirements of the Act.

The PWU reserves the right to maintain the confidentiality of those who contribute to any research or project where appropriate and to preserve their anonymity.

The PWU upholds the rights of individuals to access to their personal records.

The People and Work Unit is committed to providing ICT equipment and ongoing training to all its staff, volunteers and learners, updating its systems as necessary to keep up with latest developments. All staff are made aware of the principles of good practice in data protection. Staff training in the use of ICT and data protection is under constant review.

DATA PROTECTION PRINCIPLES (as specified by the Data Protection Act 1998)

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that or those purposes
3. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
7. Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of or damage to personal data
8. Personal data shall not be transferred to a country or territory outside the European Union 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.

People and Work Unit Data Security Policy

- Access to all Unit computers is pass-word protected and pass-words changed regularly
- Confidential files are stored with access prohibited to all but the named user
- All computers lock off after ten minutes inactivity
- All computers are protected by anti-virus software that is continuously updated
- All the Unit's paper documents are scanned into the computer and saved on archive files to protect against theft or fire loss or damage
- All remaining paper-based data is stored in locked filing cabinets and access to them is controlled
- All electronic data is backed up on a separate server and data up to three days old is stored off the premises
- All personal records are regularly reviewed and updated; unnecessary or outdated data is deleted
- All data is insured through the Unit's office insurance policy
- All non-office staff are required to:
 1. keep all IT equipment password protected and secure from unauthorised scrutiny
 2. keep all IT equipment secure from theft
 3. keep confidential and secure all personal information about colleagues or volunteers unless authorised to do so by a line manager or the Director of the Unit in the course of your work