

October 2010

# PEOPLE AND WORK UNIT

## ICT POLICY

*(this document forms part of the People and Work Unit Employment and project pack)*

### GENERAL STATEMENT

The People and Work Unit is committed to providing ICT equipment and ongoing training to all its staff, volunteers and learners, updating its systems in line with latest developments. It provides access to PCs, laptops, printers, scanners, digital cameras, video cameras, Powerpoint presentation units and any other items necessary for the efficient running of the Unit and the training of its staff and learners. How ICT will be used and staff training in ICT are under regular review and are included in all project planning.

### SPECIFICS

In addition to gaining qualifications relevant to the project on which they are working, employees will:

- have IT training to enable them to produce quotations, keep accounts, send and receive email and access the internet, including formal qualifications such as OCN units or the ECDL, as required
- have access to the above equipment to assist in presentations and assignments
- some will have access to a laptop computer to enable them to complete assignments and carry out on-line research

### SECURITY

- Access to all Unit computers to be pass-word protected and pass-words changed regularly
- All data stored on the core Unit server to be backed up twice weekly and stored off the premises
- Confidential files to be stored with access prohibited to all but the named user
- All computers to lock off after ten minutes inactivity
- All computers to be protected by anti-virus software that is continuously updated
- All personal records to be regularly reviewed and updated; unnecessary or outdated data to be deleted or securely archived

- All the Unit's paper documents to be scanned into the computer and saved on archive files to protect against theft or fire loss or damage.

All staff are required to:

1. keep all portable IT equipment password protected and secure from unauthorised scrutiny
  2. keep all portable IT equipment secure from theft
  3. adhere to the requirements of the Data Protection Act 1998 in respect of the processing and storing of personal data
- All data to be insured through the Unit's office insurance policy

## **EMAIL AND INTERNET USE POLICY**

The use of email by Unit staff is encouraged where such use supports the Unit's goals and objectives. However, employees must ensure that they:

- Comply with current legislation
- Use email and use the internet in an acceptable way
- Do not create unnecessary risks to the Unit by misuse of the internet or of email

### ***Unacceptable email and internet use***

- Use of Unit communication systems to set up personal businesses or send chain letters
- Use of computer to perpetrate fraud, or software, music or film piracy
- Forwarding of Unit confidential messages to external locations
- Accessing and/or downloading copyrighted information in a way which violates the copyright
- Accessing internet sites or distributing or storing images, text or material that might be considered indecent, pornographic, obscene or indecent
- Distributing or storing images, text or material via email, 'blogs' or internet sites that might be considered offensive, discriminatory or abusive, in that the context is a personal, sexist or racist attack, or might be considered as harassment
- Breaking into the Unit's or another organisation's system or unauthorised use of a password/mailbox
- Broadcasting unsolicited personal views on social, political, religious or other non-work related matters
- Revealing confidential information about the Unit in a personal on line posting, upload or transmission, including financial details or information regarding staff, beneficiaries, policies or internal discussions
- Transmitting unsolicited advertising or commercial material

- Undertaking deliberate activities which waste staff effort or networked resources
- Introducing any form of computer virus or malware into the Unit's network
- Installing any unauthorised software

**The Unit maintains the right to monitor software in order to check on the use and content of emails. Such monitoring will be undertaken in accordance with a procedure agreed with employees.**

Where it is believed that an employee has failed to comply with this policy, they will face the Disciplinary Procedure (see Disciplinary and Grievance Procedures Policy in the Employment Pack). The actual penalty applied will depend on the seriousness of the breach and the employee's disciplinary record.

***Agreement***

I understand and accept this policy

***Signed***.....

***Date***.....