

# Standards of Behaviour at Work - the Use of IT Systems

## 1. Introduction

1.1 This policy should be read in conjunction with the University's policy statements on 'Dignity at Work'. This policy contains two strands: ‘Standards of Behaviour at Work’ and ‘Workplace Relationships’.

1.2 The University believes it is important that staff have a clear understanding of the expectations that the University places on them and the standards to which they are expected to work. These relate both to the work they undertake and the way in which they conduct themselves at work.

1.3 The significant growth in the use of IT in the workplace has led to the development of new working practices for many staff. Future technological developments will further influence and change the workplace and will require staff to continue to demonstrate a positive and flexible response. This document outlines the expectations placed on staff in relation to their use of IT systems in the workplace.

## 2. Approach

2.1 The underlying philosophy is that the University's computing facilities should be used in a manner which is ethical, legal, appropriate to the University's aims. IT facilities must be used in a manner which does not obstruct the work of others and which encourages a scholarly atmosphere to be maintained. The system is a shared resource and each user has responsibility to learn how to use it appropriately. The University encourages the use and exploration of its IT system but discourages behaviour which may inconvenience other users.

2.2 IT facilities includes all computer systems and/or computing hardware and software (including associated peripherals) made available by the University.

## 3. Scope

This policy applies to all users of IT facilities in relation to;

• The use of computing devices

• IT facilities owned, leased, hire or otherwise provided by the University, connected directly or remotely to the University's network or IT facilities, or used on the institution's premises, or individuals connecting their equipment to the network i.e. personal laptops

## 4. Access to and the Use of IT Facilities

4.1 No one may use IT facilities without prior registration.

4.2 Registration to use the University's IT facilities constitutes acceptance of this policy.

4.3 Users are given access to those parts of the system which are appropriate to their role. Users are therefore not normally expected to seek access to other parts of the system unless authority is given. Unauthorised access to data is not acceptable and may result in disciplinary action.

4.4 The granting of access rights to IT facilities will be by the provision of access cards, user IDs and passwords giving access to locations, hardware and/or software facilities. The provision of such user references and passwords will constitute access rights for the use of those IT facilities under the conditions applicable to those facilities.

4.5 Staff must notify IT Services of any change in their duties which may affect their access and right to use IT facilities.

4.6 Users of IT facilities are expected to comply with the conditions of use which include the following. Users must not:

• disclose user id’s, personal passwords which give access to the system (NB personal passwords should be changed regularly)

• enable unauthorised third party access to the system

• deliberately damage IT equipment

• delete, amend or otherwise corrupt the data or data structures of other users without their explicit permission

• knowingly introduce viruses or other harmful programmes or files

• connect to any internal IT facility without the permission of the appropriate manager

* attempt to gain deliberate unauthorised access to external facilities or services

• use the IT facilities to send unsolicited, unauthorised commercial or illegal advertising or other material

* load software for which no licence is held
* modify software
* use the IT facilities of the University for commercial gain without the explicit permission of the appropriate authority.

4.7 Much of the information held on the University's IT system is confidential and must not be disclosed to other parties. Should staff be in any doubt about disclosing information, then they should seek advice from their manager or other appropriate managers.

4.8 The Data Protection Act 1998 outlines the legal position in relation to the use of data. Users who would like advice about the content or implications of this Act should contact Personnel Services, or Bill Marshall, Director of Finance, the University's Data Controller.

## 5. Equipment

5.1 Users are responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use to make their use safe and effective.

5.2 No equipment or other IT facility may be moved without the prior agreement of IT Services.

5.3 No equipment may be connected to the University's networks without the prior agreement of IT Services.

5.4 Serious damage or the theft of IT equipment should be reported to the University's security staff who will advise the University’s Insurance Officer and IT Services.

## 6. The Use of E-Mail

6.1 The use of electronic mail (e-mail) has grown significantly to the extent that it now represents an important means of communication both inside and outside of the University. The e-mail system can be accessed by all users whose role and responsibilities require them to use the computing network. Its use is therefore extensive and hence it is important that all of its users recognise that, whilst such a system can have many benefits, there are also limitations.

Users should note that e-mail is considered by the University as a standard communication mechanism. Those staff who are given access to the system will therefore be expected to access the facility as regularly as necessary to send and receive information.

6.2 E-mail is a fast and convenient means of communicating information. However because of this there may be a temptation not to take sufficient care when initiating messages and sending replies. It is important that users recognise the need to pay the same care and attention to the composition of e-mail messages as to other forms of written communication. An informal communication may be appropriate in some circumstances, for example when communicating with colleagues on an informal topic. It will not however be appropriate when the issue is more formal orwhen communicating externally. Care should be exercised in constructing messages, for example, the use of capitals is considered to be the equivalent of shouting. E-mail lacks the cues and clues that convey the sense in which what you say is to be taken, and the wrong impression can easily be conveyed.

6.3 E-mail is a valuable means of communication and can be the most appropriate mechanism in a variety of circumstances for example, for short memos, when the purpose of the communication is to convey straightforward information, where speed of communication is important and where a consistent message to a number of people is required. However there are also a number of situations where it is unlikely to be the most appropriate, for example;

* when the information to be communicated is complex and/or lengthy
* when discussion about a topic is likely to be necessary and hence face to face contact is more appropriate
* when a signature is required on a communication

6.4 E-mail should not be used;

* where the type of information being communicated is such that it would be better conveyed face to face or in writing. This could include information of a sensitive, personal or confidential nature. It should also be remembered that there is inevitably an increased risk of information sent via e-mail being misdirected.
* as a substitute for conveying information personally when this would be more appropriate.

The e-mail system should not be used as a means of storing important information.

6.4.1 When e-mail is used to communicate simple messages to all staff it must be supplemented by some other form of communication for those categories of staff who do not have access to a computer in their daily activities.

## 7. Unacceptable Behaviour

7.1 Unacceptable behaviour in relation to the use of IT systems will not be tolerated and where it is identified there are a range of informal and formal routes which may be followed including disciplinary action where necessary.

Some forms of behaviour will always be considered to fall below the standard of acceptability. These include;

* the use of inappropriate language in communications
* sending inappropriate messages including those which are discriminatory, sexually harassing or offensive to others on the grounds of race, disability, gender, religion or sexual orientation.
* the sending of potentially defamatory messages which criticise other individuals or organisations (legally e-mail is classified as a form of publication, governed by the rules of disclosure, libel and employment law).
* the creation, display, production, circulation or transmission in any form or medium of inappropriate material, such as pornographic or other offensive material from the Internet.
* forwarding confidential, sensitive or personal information onto 3rd parties without gaining appropriate consent
* using the IT system for commercial gain
* overloading the system by sending inappropriate bulk messages
* sending messages which are rude, overbearing, aggressive or bullying

7.2 Users have a responsibility to ensure that copyright and licensing laws are not breached when composing or forwarding e-mails, e-mails attachments and using the Internet. The laws regarding breach of copyright apply equally to the downloading and copying of information from the Internet. Staff must be clear whether there is an entitlement to download information before using and disseminating this.

## 8. Contracts

Users should be aware that enforceable contracts may be formed over the internet and e-mail and staff should therefore take care to avoid entering into any written commitments which might be legally binding where they do not have the appropriate authority to do so.

## 9. Other forms of IT systems

The University uses surveillance equipment, in accordance with the Data Protection Act, in order to ensure the safety of its staff and security of its property. The University recognises the right of individuals to privacy and hence use of this equipment is restricted and would only be used for other purposes after appropriate staff had been advised of the intention to do so.

## 10. Electronic Signatures – UWE security protocol

10.1 No electronic signature may be used without authorisation from the signatory , which may be given generally (in which case in must be in writing and signed otherwise than electronic signature) or specifically, for example when contained in a print order request. In the case of a print order request the request must include a valid cost code.

10.2 No electronic signature shall be used except for the purpose for which it was authorised, and in accordance with the terms and conditions of the authorisation.

10.3 The Head of Printing and Stationery shall ensure that no-one has access to scanned signatures held at Printing and Stationery except on the instruction of a senior member of the University such as The Production Manager, The Systems Manager or the Printing and Stationery Manager. .

10.4 The Head of Printing and Stationery shall ensure that the retrieval system is protected by password and such other security measures as the Head of Information Technology Services may advise from time to time.

10.5 Provided these regulations are complied with by the authoriser, the University will indemnify the authoriser against all costs, claims, actions and demands that may be made against the authoriser as a result of unauthorised use of the electronic signature by persons employed or engaged by the University.

10.6 Any unauthorised use of signatures, electronic or otherwise, will be treated by the University as a breach of the employee’s contract of employment and may be made the subject of disciplinary proceedings, apart from any civil or criminal proceedings that may be instituted under the Computer Misuse Act or otherwise.

## 11. Personal Use of the IT System

The majority of staff need access to the University's IT facilities in order to be able to fulfil the responsibilities of their role. The prime purpose of access to these facilities is therefore work related. Excessive personal use of the University's IT systems is not acceptable. Monitoring of individual usage of the IT facilities will not be undertaken as a matter of course. However this may be necessary when concerns arise about the level or nature of personal use of the systems. Disciplinary action may be considered appropriate in such circumstances.

## 12. Taking Action

12.1 The 'Standards of Behaviour at Work' policy statement is contained within the policy ‘Dignity at Work’ and outlines the action that will be appropriate when problems with behaviour have been identified. This ranges from informal action through to formal disciplinary action and will depend on the nature of the issue. In the majority of cases informal action will be most appropriate. There will be some circumstances, such as when the behaviour might constitute a disciplinary offence, when formal action may be necessary, in which case a formal investigation will occur. Disciplinary action may then be appropriate depending on the outcome of the investigation.

12.2 Even where a formal complaint is investigated locally and there is no disciplinary action taken as a result, Personnel Services must be notified of all such complaints to ensure consistency of approach and decision making throughout the University.

12.3 The use of IT facilities and data is subject to relevant legislation.

## 13. Sources of Advice and Assistance

Several sources of advice have been identified in this statement. Further recommendations on sources of assistance are given in the 'Dignity at Work - Standards of Behaviour at Work' policy statement.

14. Any queries about this policy statement should be raised with Personnel Services or IT Services as appropriate.

15. The University reserves the right to change this policy from time to time as may be deemed necessary.