

# COMPANY OR ORGANIZATION NAME

## E-MAIL & INTERNET POLICY

### 1. Introduction

Company Name recognizes that Internet and e-mail systems have the potential for enormous benefit to Company employees, but can be misused.

This policy explains what is classified as the acceptable and unacceptable use of the Internet and e-mail systems at Company Name.

All employees using the Internet and e-mail at work must comply with the Company Regulations pertaining to the Use of Information Technology Facilities (Appendix 1) and the Acceptable Use Policy(Appendix 2).

Breaches of this policy will be dealt with through the Company's Disciplinary Procedures for students and staff. These will be implemented at a level appropriate to the seriousness of the alleged misconduct.

### 2. Regulations of Investigatory Powers Act 2000, Data Protection Act 1998 and The Human Rights Act 1998

The Company encourages the use of the Internet and e-mail systems and is committed to acting in compliance with individual's rights under both the Human Rights Act 1998 and the Data Protection Act 1998. While the Company routinely monitors the overall patterns of e-mail and Internet usage it does not, in the normal course of events, specifically identify the use made of the facilities by any individual employee.

However, under the Regulations of Investigatory Powers Act 2000, e-mail and Internet systems are subject to random monitoring and recording by or on behalf of the Company. Accordingly, while the Company will at all times seek to act in a fair manner, employees should be aware that there can be no legitimate expectation of privacy when using the Company's e-mail and Internet facilities.

### 3. Application

The following procedures apply to all electronic media and services which are;

- accessed on or from the Company's premises,
- accessed using the Company's computer equipment, and/or
- used in a manner which identifies the individual with the Company,
- accessed remotely e.g. from home, or while traveling on Company business

Any third parties such as visitors, agents or consultants using the Company Internet or e-mail services will also be subject to compliance with this policy. All applications for use of the Company Staff e-mail system by third parties (visitors, agents, consultants, suppliers) shall be authorized by \_\_\_\_\_.

It is the responsibility of the employee who authorizes third party use to ensure that third parties have read and understood the terms of this policy and agree to be bound by it. In addition, third parties will read, understand and confirm their agreement to be bound by it, by signing the appropriate forms (appendix 4).

#### **4. Legal Liability**

##### **1. Employees**

Employees should be aware that legal responsibility for employee e-mails and for Internet misuse by an employee rests with both the Company and the employee responsible. For instance, where an email contains a defamatory comment or a comment which could be considered to amount to sexual harassment then this could attract liability to both the author of the email and to the Company. Accordingly, employees should be aware at all times that responsibility for e-mail and Internet misuse lies wider than the individual who misuses it.

Similarly, employees should be aware that the Company can be held to be vicariously liable for representations made of contractual arrangements entered into by its employees where it is reasonable for a third party to assume that the employee is acting with the Company's authority. Heads of Departments and other Senior Staff should take great care in relation to both external and internal e-mails which could be contractually binding.

#### **5. Security**

##### **1. Staff**

Staff must respect the confidentiality of employees' electronic communications and must adhere to the regulations in the "The Company Regulations pertaining to the Use of Information Technology Facilities" (Appendix 1).

#### **6. Software**

Employees will not use the Internet to download entertainment software or games, to play against others across the Internet or participate in online gambling. Employees must not

download software which may be used to “sniff” the Company Network in order to determine employee passwords or to enable hacking into the Company systems.

## **7. Viruses**

The Company’s Virus Policy is attached (Appendix 3).

## **8. Defamation**

Employees must not write, send, publish, copy, distribute or forward derogatory or defamatory remarks about any person or organization either on the Internet or by e-mail. If an employee discovers potentially defamatory material, then they should report it to their manager immediately. If an employee discovers potential defamatory material they should report it to their immediate supervisor or Head of Division. Employees must not send or forward discriminatory messages, even if it is intended as a joke, as this could be regarded as harassment.

## **9. Offensive Material**

AS stated in the “Company Regulations pertaining to the Use of Information Technology Facilities” it is unacceptable to access, archive, store, distribute, edit or record sexually explicit or other offensive material. The display of any sexually explicit image or document is unacceptable. This includes screensavers. The display of such material can result in claims of harassment and discrimination and will risk disciplinary action and implementation of the Company’s Disciplinary Procedure.

An employee who inadvertently finds that they have accessed a site containing offensive or sexually explicit material must exit the site immediately. If an employee is found to be accessing such sites regularly (more than once) then they will risk disciplinary action and implementation of the Company’s disciplinary procedure.

An employee who receives unsolicited, offensive or sexually explicit e-mails should inform their line manager / Head of Division. It will be for the manager or Head of Division to decide whether further investigation or disciplinary action is appropriate.

Unsolicited material which is circulated internally or externally, which has its origin internally or externally, may be classified as SPAM. Any employee who is found to be the originator of a SPAM attack from within the Company, using Company equipment will be subject to disciplinary action by the Company.

## **10. Illegal Use**

An employee who is found using the Internet for illegal purposes will be subject to the Company’s Disciplinary Procedure and, in addition, may be reported to the police.

10.1 The use of IT facilities is subject to provisions of the following acts as stated in the Company Regulations pertaining to the Use of Information Technology Facilities

10.1.1 Data Protection Act 1998

10.1.2 1998 Telecommunications Act 1984

10.1.3 Copyright, Designs and Patents Act, 1988 and subsequent regulations

10.1.4 Computer Misuse Act, 1990

10.1.5 Computer Copyright Software Amendment Act 1985

10.1.6 Criminal Justice and Public Order Act 1994

10.1.7 Race Relations (Amendment) Act 2000

10.1.7 Human Rights Act 1998

10.1.8 Regulation of Investigatory Powers Act 2000

10.2 Compliance with Copyright

Employees may not download copyright materials from the Internet unless they have documentary evidence of proof of purchase or right to use. This includes copyright MP3 files, books, diagrams, photographs etc. If such materials are required for Company purposes, the copyright law surrounding the use of such materials must be investigated and compliance ascertained and documented before materials are used.

10.3 Plagiarism

Employees may not access Internet sites in order to download material which is known or subsequently found to be plagiarized.

## **11. Acceptable Personal Use of E-mails**

11.1 Company E-mail System

Electronic media and services are primarily for Company business use. Limited, occasional or incidental use of e-mail (sending or receiving) for personal purposes is understandable and acceptable where such use does not contravene this policy. Employees should make it clear the e-mail is a personal communication and not on behalf of the Company. The

Company will not tolerate employees who spend lengthy periods of their working day using the e-mail system for non-work related purposes. Staff who abuse the e-mail system risk disciplinary action.

The Company's e-mail system must not be used to send personal e-mails where there is a real risk of a personal communication being interpreted as a communication made on behalf of the Company.

The Company e-mail system, or any other e-mail system accessed via the Internet using Company equipment or systems, must not be used to send or circulate copyright material unless appropriate permission, and/or payment for use have been obtained / carried out and proof of purchase or authorization to use is held.

In accordance with the Company Regulations pertaining to the Use of Information Technology Facilities personal e-mails must not be used to send junk e-mails or unsolicited marketing material (SPAM) which can overload systems and disrupt e-mail services with a consequent impact on costs; such prohibited material can include chain letters and offers, hoax virus alerts, amusing animations and graphics, unsolicited mail or communication lists.

## **12. Acceptable Personal Use of Internet**

Limited, occasional or incidental use of the Internet for personal purposes is understandable and acceptable where such Internet use not contravene this policy. However, in allowing this, the Company requires employees to act responsibly. Employees must never allow use of this facility to interfere with their job performance or work responsibilities. Staff who abuse this privilege will be subject to disciplinary action. If staff use the Company Internet access system to carry out on-line transactions, the Company takes no responsibility for any part of the transaction and is not liable for any failure of security that might occur as a result of the transaction. The Company will keep the use of this facility under review and reserves the right to withdraw the facility.

It is not permissible for goods purchased over the Internet to be delivered to the Company's address.

## **13. Confidential Data**

Accidental breaches of confidentiality can occur by entering a wrong address or forwarding a message to inappropriate recipients on the Company's distribution list. It is advisable when sending confidential or sensitive material by e-mail that you ensure that it clearly states to the recipient that it is private and confidential.

#### **14. E-mail Disclaimer**

The following disclaimer shall be added at the front of each outgoing e-mail:

“This email is confidential, may be legally privileged, and is for the intended recipient only. Access, disclosure, copying, distribution, or reliance on any of it by anyone outside the intended recipient organization is prohibited and may be a criminal offence. Please delete if obtained in error and e-mail confirmation to the sender.”

#### **15. Best Practice Guidelines for the Use of E-mail**

E-mail communications are often perceived as being closer to informal speech rather than formal writing. E-mails can be sent quickly and often with little thought regarding their contents. What the sender may construe as acceptable could be construed as rude and abrupt by the recipient.

Therefore, the following best practice guidelines should apply when sending e-mails:

1. “GCU All” e-mails should not be sent unless it is intended to reach every member of staff in the Company with access to electronic systems.
2. Never say anything in an e-mail that you wouldn’t say face to face. Correspondence by e-mail should never be used as an alternative to replace communicating with another employee in person.
3. The inappropriate use of upper case in e-mail is generally interpreted as SHOUTING and should be avoided.
4. Messages should be concise and to the point. Employees should not send heated messages (often called “flames”) impulsively or in anger.
5. Proof read e-mails before sending to avoid misunderstanding.
6. Check distribution lists before sending an e-mail and target members of staff according to how important the message is to them.

#### **16. Review**

The E-mail and Internet Policy will be annually reviewed  
by: \_\_\_\_\_

## APPENDIX 1

### Company Regulations pertaining to the Use of Information Technology Facilities

#### 1. Scope

These regulations apply to users of all IT facilities owned, leased or hired by the Company, all users of IT facilities on Company premises and all users of any IT facilities connected (locally or remotely) to Company networks.

#### 2. The Legal Framework

The use of IT facilities is subject to provisions of the following acts:

- 2.1 Data Protection Act, 1998
- 2.2 Telecommunications Act, 1984
- 2.3 Copyright, Designs and Patents Act, 1988 and subsequent regulations
- 2.4 Computer Misuse Act, 1990
- 2.5 Computer Copyright Software Amendment Act 1985
- 2.6 Criminal Justice and Public Order Act 1994
- 2.7 Race Relations Act 1976
- 2.8 Human Rights Act 1998
- 2.9 Regulation of Investigatory Powers Act 2000

Users must comply with any regulations and instructions displayed alongside IT facilities.

#### 3. Authorization

Use of any IT facility is open only to staff Company of the Company , and other persons authorized by the 'designated authority', that is the \_\_\_\_\_

#### 4. Registration

Use of certain of the facilities is conditional upon prior registration and the allocation of a user identification reference authorized by the designated authority. The granting of a

user identification reference will constitute the authorization for the use of facilities referred to in paragraph 3.

## 5. Access

IT facilities will have access times posted in a prominent position. Employees may not occupy any IT facility outside the permitted hours of access.

## 6. Conditions of use for hardware and software

1. Users must not in any way deliberately cause any form of damage to Company computing equipment or software, or to any of the rooms which contain that equipment. The term 'damage' includes modifications to hardware and software which, whilst not permanently harming the hardware or software, incurs time and / or cost in restoring the system to its original state. Any costs associated with repairing or replacing deliberately damaged equipment or software and / or in providing temporary replacements will be determined by \_\_\_\_\_.
2. Users must adhere to the terms and conditions for all license agreements relating to any part of those facilities including software, equipment, services, documentation or other goods.
3. Users must not copy software or documentation without permission from the designated authority.
4. Users must not modify any software or incorporate parts of any software into their own work, without permission from \_\_\_\_\_ . , t
5. Users must comply with any instructions or regulations displayed alongside computing facilities.
6. Users must not deliberately introduce any virus, worm, Trojan horse or any other 'nuisance' program or file on to any system external or internal to the university or take deliberate action to circumvent any precautions taken by the Company to prevent 'infection' of its machines.
7. Users must not delete other users' files or interfere in any way with the contents of their directories.
8. Users must not use another user's identification reference or allow another user to use his / her own reference.

9. Users are responsible for maintaining the security of their own password. Should they divulge the password to anyone else, they will be accountable for the use of their account by that person.
10. Users must not make use of any of the Company's computing equipment to connect to any other computing facilities or commercial services without prior permission and appropriate registration. Application for such permission must be made to \_\_\_\_\_.
11. Every user of networking facilities must observe any standards or rules relating to use of the networks and / or computer systems to which he / she has access over those networks.
12. Users must not connect any non-standard device into the Company's network without prior written agreement from \_\_\_\_\_.
13. Users must ensure that they terminate each session in accordance with published instructions.
14. Users must comply with the guidelines issued in accordance with published instructions.
15. Users must not use e-mail services to forge e-mail signatures or harass any other person external or internal to the Company.
16. Users must not use IT Services to store, produce, transmit or display text of images that could be considered to be offensive e.g. sexual, pornographic, racial abuse, libelous, of terrorist nature or to make others fearful, anxious or apprehensive or that could bring the Company into disrepute.

## **7. Behavior**

1. Users can be held accountable for any cost or inconvenience caused by the excessive use of network bandwidth for activities that are not in accordance with the Company Acceptable Use Policy. The Company reserves the right to decide on any cost or inconvenience caused.
2. Smoking, eating or drinking is not permitted in any Company computer lab.
3. Users must respect the rights of others and should conduct themselves in a quiet and orderly manner when using IT facilities. Users must not occupy a computer workstation unless they are actively using it for bona fide purposes.

4. The playing of unauthorized computer games is not permitted. The use of Internet facilities, (e.g. Web surfing, Chat, E-mail), for purposes that are not directly related to Company activities is not permitted during busy periods.
5. No equipment should be removed from its designated place or be tampered with in any way. This includes changing workstation characteristics.
6. Interference with or removal of printout which belongs to another person is not permitted.
7. Stationery should only be used for the purpose for which it is supplied. It should be carefully conserved and unused stationery should not be removed.

#### 8. **Equipment Loans**

1. No equipment or software may be borrowed without the agreement of the \_\_\_\_\_.
2. Any software or equipment borrowed as part of a formal loan scheme or for the duration of a particular project must be returned on the date agreed at the time the loan was made.
3. All reasonable care must be taken to ensure the security of any equipment while in their possession.

#### 9. **Private and Commercial Use**

1. The use of any Company IT facilities for commercial gain or for work on behalf of other groups is not permitted unless prior agreement has been made with \_\_\_\_\_. An appropriate charge for that use will be determined and agreed before any work is carried out.
2. The use of the Company's IT facilities for reasonable purposes is permitted, as determined by \_\_\_\_\_.

#### 10. **Charging**

There may be a charge for use of certain facilities. Failure to pay outstanding charges may result in withdrawal of services and / or withholding of compensation.

#### 11. **Disclaimers**

The Company accepts no responsibility for the malfunctions of any equipment or software, failure in security or integrity of any stored program or data or for any loss alleged to have been caused whether by defect in the resources or by act or neglect of the Company, its employees or agents.

## **12. Disciplinary Procedures**

The use of Company IT facilities will be monitored to ensure compliance with these regulations.

Failure to observe these Regulations for the use of IT facilities may result in the following procedures being involved:

1. Application of Company disciplinary procedures
2. Withdrawal of access to IT facilities, locally or across the Company
3. Serious offences may be reported to the police for further investigation and possible prosecution

## **APPENDIX 2**

### **Acceptable Use Policy**

1. An employee may use Company Internet and Email for the purpose of inter-working with other user Company employees.
2. Subject to the following paragraphs, Company Internet and Email may be used for any legal activity that is in furtherance of the aims and policies of the Company.
3. The Company Internet and Email facilities may not be used for any of the following.
  1. Creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images of material.
  2. Creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
  3. Creation or transmission of defamatory material.

4. Transmission of material such that this infringes the copyright of another person.
5. Transmission of unsolicited commercial or advertising material either to other User Organizations, or to organizations connected to other networks, save where that material is embedded within, or is otherwise part of, a service to which the member of the User Organization has chosen to subscribe.
6. Deliberate unauthorized access to facilities or services accessible via the Company Internet and Email facilities
7. Deliberate activities with any of the following characteristics:
  1. Corrupting or destroying other users' data
  2. Violating the privacy of other users
  3. Disrupting the work of other users
  4. Using the system in such a way that denies service to other users, for example, the deliberate or reckless overloading of access links or of switching equipment)
  5. Continuing to use an item of networking software or hardware after the Company has requested that use cease because it is causing disruption to the correct functioning of the Company
  6. Other misuse of the system or networked resources, such as the introduction of "viruses"
4. Where the Company Email and Internet system is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use the Company Email and Internet system.
5. A third party, where an individual, means someone who is not acting as a member of the Company. Where it applies to a separate organization, this is defined to be any organization that is in law a separate entity to the Company.
6. It is the responsibility of the Employee to take all reasonable steps to ensure compliance with the conditions set out in this policy document, and to ensure that unacceptable use of Company systems.

## APPENDIX 3

### Information Technology Virus Policy

1. A comprehensive centrally based virus monitoring system has been set up to detect current known viruses and facilitate their removal. The virus monitoring system continuously scans all e-mails entering the Company. Every PC attached to the Company network has virus checking software installed to ensure that all documents are scanned for viruses before use. The software is also configured to ensure that full system scans are carried out regularly and automatically.
2. Industry standard anti-virus software packages are procured centrally for all platforms connected to the network. The packages, and their latest updates, are available from \_\_\_\_\_ centrally managed networked servers. It is the responsibility of the administrator of each system to ensure that the latest version of anti-virus software is loaded onto systems for which they have responsibility. IT staff will provide assistance upon request.
3. All software installed on network connected systems will be purchased from known reputable suppliers and must be received in the original manufacturers' packaging. IT Helpdesk will help staff to purchase software where it is possible to obtain significant discounts.
4. Back up copies of core and corporate software applications will be stored in a safe 'off-site' location.
5. All new software will be virus checked by IT staff before being installed on network connected systems.
6. Systematic backup of central systems and software will be made to allow restoration of a system that has been infected by a 'time release' virus. It is the responsibility of individual users to backup data files.
7. Programs and data will be made available on a 'need to use' basis. This will ensure that problems are isolated, critical applications are protected and it will facilitate problem diagnosis.
8. Users will not be permitted to use their own copies of software on network connected systems unless explicit written permission is obtained from the IT Manager responsible for that system.

9. Viruses can be transferred by downloading documents from the Internet or from e-mail attachments. In order to minimize the risk associated with use of data from external sources it is vital that all staff ensure that the latest version of anti-virus software is installed on computers for which they are responsible.

### **Action in Event of Infection**

1. Any hardware / software showing symptoms of possible infection will be removed by IT staff and all data on the machine(s) in question will be backed up immediately. Users can assist IT staff by reporting any suspected viral problems immediately to the IT Helpdesk.
2. Any employee of the Company implicated in the deliberate introduction of a virus, or the accidental introduction of a virus through failure to adhere to the preventative measures detailed above will be subject to Company disciplinary procedures.

### **Guidance**

The following guidance will help reduce the risk of infection:

1. Always scan 'foreign' floppy disks, CD's and DVD's before using them for the first time.
2. Always scan files downloaded via the Internet before running any programs.
3. Never boot a PC from a floppy disk unless you are certain that it is virus free.
4. Use the write protect features on floppy disks and writeable CDs or DVDs whenever possible.
5. Only use licensed copies of software obtained from a reputable source.
6. Do not install any new software on the PC unless it has been virus checked by IT staff and verified "clean".
7. Use password protection whenever it is available (PCs or network connections) to prevent unauthorized access to files.
8. Make regular backups of all important work and store them securely.

9. Don't panic and don't propagate unsubstantiated information about virus infection.
10. Re-format a diskette when it is to be re-used or re-cycled

**APPENDIX 4**

**Authorization of Visitors, Agents and Consultants to use University Systems**

I .....(insert name) hereby acknowledge that I have received a copy of the Company policy for use of e-mail and Internet use including the Acceptable Use Policy, the Company Virus Policy and the Company Regulations pertaining to the Use of Information Technology Facilities. I agree to be bound by these regulations and policies.

Name	(print name)
Signature	
Date	
Place of work	
Contact telephone no	
E-mail address	
Details of systems to be accessed (include name, module or area, and level of access)	
Access required	From (enter date): To (enter date):

**Approval for Use**

Proposed by	(print name)
Signature	
Date	
Approved by :	(print name)
Signature	
Date	

Please send a copy of this form fully signed to the \_\_\_\_\_, copied to the IT Helpdesk in order that access to Company systems can be enabled.

In order to ensure that access is enabled for arrival or start date please submit forms at least one week in advance.

Sample Preview  
Sample Preview