Policy on Computing and Telecommunications Usage

1. Introduction

In October 2000 the Human Rights Act 1998 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (made under the Regulation of Investigatory Powers Act 2000) came into effect. Together they have focused on the issues of an employee’s privacy and the employer’s right to monitor communications on its telecommunications systems.

The purpose of this policy is to set out what is acceptable use and the general conditions of when monitoring by the University may occur.

2. Acceptable Use

All communications made on University systems remain the sole property of the University and should be used primarily for business related purposes.

Computing facilities and telecommunications, including fax, telephones, email, and access to the Internet, are provided for the better performance of the person’s duties, and not for social usage. Excessive personal / social use is likely to be picked up by monitoring of individual usage (See 4 and 8).

Inappropriate use of the University’s IT equipment and systems will lead to disciplinary action and may result in dismissal.

3. Email

You must ensure that emails, which you are sending internally or externally, comply with the University’s Policies.

In particular you must not:

1. Send offensive email. The sender of an email which, causes offence is subject to the normal disciplinary procedures. In this respect a problem arising from email is no different from any other interpersonal dispute. However, unlike purely verbal communications, it is possible to supply evidence to support a complaint. Offensive email could encompass all or any of the forms of harassment, discrimination and bullying.
2. Knowingly make any inaccurate or defamatory statement in your email messages (or other correspondence). If you have any doubts about the advisability of the subject matter or phraseology of your email message, do not send it, or seek advice from your supervisor before doing so.
3. Indulge in excessive use of email for personal and / or social purposes.
4. Infringe a third party’s intellectual property rights by sending protected material without crediting the owner.
5. Send malicious email messages.
6. Imply that your message contains the official policy, view or intent of the University if it does not.
7. Send confidential information via email, unless this is **essential** to your work. Messages can fall into the wrong hands, for example simply by a recipient inadvertently forwarding to another; users should always be aware of the potential for confidential material to be mis-directed.

University email going off-site should carry the official disclaimer verbatim, where possible added by the mail program or the sender.

The University recognises that unsolicited email (spam) is a significant nuisance and will take every reasonable precaution against it. University email users will not generate spam by sending out unsolicited mass emails. Incoming messages that are likely to be spam will be identified and marked as such in their subject headers. Although the most appropriate software available will be used, this process can still give false results, so no messages will be deleted. The intention is to forewarn recipients to use their judgement to delete suspect messages without opening, thereby avoiding the risk of exposure to unsavoury or non-work related material that they may contain. The University seeks to protect staff from such exposure as much as possible, so if you have any doubt about a suspect message do not open it but seek advice from your supervisor.

### 4. Internet Access

You may use the Internet to access and download acceptable material for work use. However you should not spend excessive time using the Internet for personal use and it should not in any way interfere with the performance of your job.

The University reserves the right to monitor network traffic, to ensure that its equipment is not being used for inappropriate purposes. This includes, but is not restricted to, any sexually explicit or violent material or sites which promote racism or intolerance.

In particular you **must not:**

1. Access, download, store or forward offensive, obscene or indecent material, be it text and / or images from any system on the Internet, such as via the World Wide Web. This is strictly forbidden, and anyone found doing so could be liable to criminal proceedings as well as any action the University may deem necessary.

2. Attempt to gain unauthorised access to any computer system of the University or any other organisation.

3. Download executable files for non-work related purposes. This includes programs, applications, utilities, screen savers, games etc. Where files are required for work purposes, the appropriate care to guard against virus infection must be taken, and registration and / or payment for the software must be made where appropriate. (Reference A)

4. Download video clips, view real-time cameras or listen to music, voice and sound streamed services for recreational or social purposes.

5. Download or use in situ any data, programs or other software or system facilities in a manner that breaches the licence agreement between the University and the service provider. It is the responsibility of every user to be familiar with licence conditions, and if in doubt to verify the position with Computing Services, or the Library, etc. before using such services.
5. Telephones

University telephones are provided for business use. The University recognises the occasional need for staff to make or receive important or urgent personal calls on university telephones, but this privilege must not be abused. Such use and the method of payment are at the discretion of your line manager.

In particular, anyone needing to make personal premium rate calls or personal international calls must first seek the sanction of his or her line manager. The University must be reimbursed for the cost of such calls.

This policy also applies to mobile telephones that are provided by the University.

The University recognises the occasional need for staff to make or receive important or urgent personal calls on mobile telephones which they own and carry with them during working hours, but this privilege must not be abused. Use of personal mobile phones during working hours should not interfere with the performance of work duties.

In the above, the term 'call' relates to telephony services which include not only voice but also the other media that the technology is capable of processing, e.g. modem data services, text messaging and picture imaging.

6. Fax

Many of the same considerations apply to the use of the fax as apply to email, namely it must not be used for sending offensive or malicious messages, inaccurate or defamatory statements, or breach of copyright.

The official disclaimer must be included in the header page, and must not be revoked in the message.

7. Email Addresses

The corporate Heriot-Watt internet email address (e.g. J.Smith@hw.ac.uk, dp7@hw.ac.uk) is the only address the University will use for official correspondence, namely:
- Staff contacting students
- Students contacting staff
- Staff undertaking University business

If you choose, for your own convenience, to set forwarding to a different address, it is your responsibility to ensure that the address is correct and that it works.

All University mailing lists will operate only on the corporate hw.ac.uk addresses assigned to staff and students.

The University accepts no responsibility for any consequences that may arise from failure to set a correct forwarding address.

8. Monitoring of Email and Telecommunications Systems

As has been clearly stated, the University’s email and telecommunications systems are provided for business use, and as such the University reserves the right to monitor the use of all such facilities, in accordance with University Regulation 29.
The Lawful Business Practice Regulations, which came into effect on October 24th 2000, allow organisations to monitor or record all communications transmitted over their systems without consent for the following purposes:

1. Establishing the existence of facts
2. Ascertaining compliance with regulatory or self-regulatory practices or procedures (i.e. ascertaining whether the business is abiding by its own policies)
3. Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and staff training)
4. Preventing or detecting a crime
5. Investigating or detecting unauthorised use of the business’s telecommunications system
6. Ensuring the effective operation of the system

The Regulations also authorise businesses to monitor (but not record) communications for the following purposes:

7. Checking whether or not communications are relevant to the business
8. Monitoring number of calls to confidential counselling helplines run free of charge

Any monitoring that the University undertakes will comply with those Regulations, and one of the purposes of the publication of this policy is to give the required notice to staff that monitoring and interceptions may take place.

9. Further Information

Further information may be obtained from the following sources:

A. Regulation 29, Conditions of use of the University Computing Facilities: User Document Gen/036
B. University Data Protection Policy
C. University Policy on Staff Records
D. Electronic Mail at Heriot-Watt: User Document Gen/156
E. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000: HMSO
F. Corporate IT Security Policy.