Conduct (Monitoring of Email and Internet Use) Policy

Purpose and Context

The University seeks to facilitate the proper and extensive use of IT in the interests of its work. This policy is intended to provide a framework for the responsible and legal use of email and internet and explains both general and specific monitoring which takes place to secure acceptable use of facilities.

All staff members using the Internet and e-mail at work must comply with the University Regulations pertaining to the Use of Computing Facilities and the JANET Acceptable Use Policy (copies available on the CLS intranet).

IT resources are provided to facilitate a staff members work. Use for other purposes, such as personal e-mail or recreational use of the World Wide Web, is allowed as a benefit to staff. Such access is not a right. Any use must not interfere with the staff members duties or anyone else's use of facilities for work purposes and must not, in any way, bring the University into disrepute.

While the University 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 staff member. However, a record of log-ins is maintained and may be considered in an investigation. Under the Regulations of Investigatory Powers Act 2000, email and Internet systems are subject to random monitoring and recording by or on behalf of the University. Accordingly, while the University will at all times seek to act in a fair manner, staff members should be aware that there can be no legitimate expectation of privacy when using the University's e-mail and Internet facilities.

Specific monitoring of the use of facilities both from examination of files held on the server and files held on an individual hard drive may be undertaken in investigating specific allegations of a breach of conduct under the University's disciplinary procedures.

---

1. Definitions of Unacceptable Use

1.1. Unacceptable use of university computers and network resources are:

- the viewing, retention or distribution of material that is offensive, obscene or indecent, except in the course of recognised research or teaching that is permitted under UK and international law
- causing annoyance, inconvenience or needless anxiety to others, as specified in the JANET Acceptable Use Policy
- defamation
- intellectual property rights infringements
- unsolicited advertising ("spamming")
- attempts to break into or damage computer systems or data held thereon
- the distribution or storage of pirated software

- non work activities which generate heavy network traffic, especially those which interfere with others' legitimate use of computing facilities or incur a financial cost.

2. Blocking and monitoring internet access

2.1. All access to the Internet is logged and monitored. If monitoring reveals possible evidence of criminal activity, or a repeated breach of the computing regulations or JANET acceptable use policy by attempting to access these sites or similar sites a disciplinary investigation will be instigated, and the police may be notified (where relevant).

2.2. Where an individual requires access to Internet sites that may contravene University or JANET acceptable use policies (such as pornography, extremism) as part of a teaching or research proposal, clearance must be obtained from the School and University Ethics Committee. This ensures that any activity identified through monitoring of Internet usage can be tied to a valid and approved activities.

2.3. Websites which are recognised as being harmful to computer systems or those known to be used to host harmful software or distribute phishing emails linked to malicious intent will be blocked to protect university systems and information.

3. Other Investigations

3.1. Where specific allegations are received relating to the conduct of the staff member the University reserves the right to check computer files held on backup files and on hard disks. In such cases the individual will be informed of the allegations and the nature and scope of the investigation being undertaken.

3.2. On rare occasions the police may request information regarding an individual's computer records. In such cases access to information will be governed by legal process.

4. Other Access Requirements or Restrictions

4.1. The use of facilities for commercial work may only be made in accordance with the Guidelines for Undertaking External Work, available in the Staff Handbook.

4.2. Individuals should not assume that the University's system is secure. If staff members use the University Internet or email access to carry out on-line transactions the University 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.

4.3. Staff members should not use another user's identification or allow another

person to use their reference. Staff members are responsible for the security of their own password and should they divulge the password to allow someone access under their own reference they will be accountable for the use of their account by the other person.

4.4. Where a staff member is absent from work for a period of time and has been unable to make file share arrangements the Dean or Director may authorise access to a staff members computer to access work related files and email.

POLICY SIGN-OFF AND OWNERSHIP DETAILS	
Document name:	Conduct (Monitoring of Email and Internet Use) Policy
Version Number:	V1.3
Equality Impact Assessment:	Completed 24/05/2018
Approved by:	Director of HR and Trade Unions via Procedures Meeting
Date Approved:	February 2022
Next Review due by:	February 2025
Author:	HR Manager
Owner (if different from above):	Director of Human Resources
Document Location:	https://www.hud.ac.uk/media/policydocuments/Conduct-Monitoring-Of-Email-And-Internet-Use.pdf
Compliance Checks:	HRG SMT regularly review to ensure compliance
Related Policies/Procedures:	Disciplinary Procedure Disciplinary Rules Staff Use of Social Media Policy

REVISION HISTORY

Version	Date	Revision description/Summary of changes	Author
V1.1	October 2016	Formatting updates (minor amends not requiring committee approval)	HR Manager
V1.2	November 2019	Formatting updates (minor amends not requiring committee approval) and transference to new template	HR Manager
V1.3	February 2022	Formatting updates (minor amends not requiring committee approval)	HR Manager