Information Technology (IT) Users Policy

(External version)

Please read this University Policy carefully which is aimed at protecting you and your use of computer systems, regarding the confidentiality, integrity and availability of information processed, stored and transmitted by them.

It applies to all users of Cranfield University IT equipment, networks and software including temporary staff and students. All users have a duty to report any information security incidents to the appropriate IT Service Desk.

If you do not follow the Policy, the consequences could be serious for you and the University:

a) We could be subject to embarrassment, loss of reputation, loss of commercial opportunity

b) You may compromise the integrity and security of the network

c) You may be subject to University disciplinary procedures

d) You may be breaking the law, which could result in civil or criminal proceedings

If you need any assistance in ensuring that your use of the University computer systems complies with the policy, please check on the intranet or speak to the appropriate IT Service Desk.

This policy will be reviewed at least annually to ensure that the contents are relevant, commensurate with the value and importance of the University's assets and ensure appropriate levels of protection of both users and IT systems.

Thank you

Professor Karen Holford — Chief Executive and Vice-Chancellor

David Ford — Director of Information Technology (IT)

1. Only nominated users may purchase, install, move and dispose of University computer hardware.

The University makes a significant investment in computer hardware to provide reliable access to IT services. University hardware must be installed, maintained, moved, and ultimately disposed of by qualified IT employees. If alternative arrangements are required, then these should be discussed with the Director of Information Technology.

This applies to all PC's, printers, computer cabling and associated University computer equipment. Mobile devices (including laptops, tablets, and smartphones) will be subject to the Mobile Device Policy.

Personal mobile devices can connect to a limited range of University services subject to adherence of the conditions in this policy.

These measures mean that assets can be easily located, assisting with technical support, and facilitating the efficient management of any proposed upgrades, whilst ensuring compliance with audit controls.

2. Only nominated users may purchase, load, and copy software used on any computer belonging to, or provided for, the University.

The University does not own the majority of commercial software used but licenses it, and the University and users must comply with the terms and conditions of all software licences. Therefore,

a) Users shall not illegally copy any software application used in the University, whether for business or personal use.

b) Users should not retain any original software unless agreed.

Audits will be undertaken to reconcile commercial software use against licenses, including restrictions on the number of users, and the ability to copy the software.

To protect yourself and the University, users of University IT equipment need to ensure that only recognised software is used. If users have any doubt about the legitimacy of a download, then they should contact the IT Service Desk for advice.

It is recognised that, although most software is installed and managed by IT, some specialist 'non-commercial' software is used directly by specific groups/departments but this use should be in liaison with the IT Service Desk to assist with support arrangements where possible.

3. Data Protection

There are specific restrictions laid down in UK data legislation regarding personal data (any information that identifies living individuals) including how it is collected and processed. For example:

a) When collecting or using data, all individuals (data subjects) must be aware as to why the information has been collected and what it will be used for i.e. 'the purpose', and the data should only be used for that purpose.

b) The University must have a legal basis for the processing of personal data, and these are detailed in the Record of Processing Activities (ROPA).

c) Personal data shall be held in-line with the University's Data Retention Schedule and will be kept secured.

d) Employees shall be aware that data subjects have a number of rights including the right to ask the University to show them all data held about them. Such requests are handled formally by the University's Data Protection Officer.

Further information can be found in the University's Privacy Policy

The University has a formal Information Handling Policy, and all information will either be categorised as Open, Confidential-Commercial or Confidential-Personal Data. Any bulk transfer of confidential data to third parties needs to be approved prior to release.

4. Don't allow unauthorised use of University computer systems & information

a) Your password provides the key to accessing the University network and the information stored on it. Keep it secure and don't let any unauthorised person use it - you may be held liable for any misuse – and don't attempt to obtain anyone else's password(s).

b) Don't use obvious passwords, such as "password" or a family name, which might be easily guessed. Use a mixture of alphanumeric characters and symbols, or a combination of three short words (known as passphrases) that meet the University Network Password Policy. Many systems automatically enforce regular password changes, but if not change your password at least every 12 months or immediately if you think someone else knows it.

c) Don't leave confidential information on an unsecured computing device, including emails and attachments, always use access controls such as 'CTRL+ALT+DEL' to lock a PC when unattended. Where necessary secure individual documents with passwords and protect appropriate confidential data with encryption when stored or during transmission.

5. Limit personal use of the University computer systems

The University computer systems, including email and internet access, are provided to support its teaching, learning, research, and administrative functions. Personal use is permitted **only** if it is occasional, reasonable and does not interfere with the performance of your duties or the academic/ business duties of others.

You must not obscure your identity when using IT facilities and you are accountable for all actions undertaken.

Please note that there is no limit on the personal use of the Residential Network by students, but all other aspects of this policy apply.

6. Remote working requires extra care

When working away from campus, you must maintain confidentiality of the University information by applying appropriate protection mechanisms and not show or disclose University confidential information to unauthorised third parties. Ensure that:

a) Any computing device is not left unattended while online, if doing so will compromise the security of information and that confidential

information is never viewed in a public place where others may see what is presented on screen.

b) You always work on data that is hosted on the University network, if possible, and avoid off-line working i.e. using the local device storage.

c) Any loss or theft of a computing device that has been used to access, and or store University information, is reported to both the IT Service Desk and appropriate office administrator.

d) Data is backed up centrally (when next available) and all software, including anti-virus protection, is updated on a regular basis.

7. Proper use of electronic collaboration/messaging services (including social media/email)

The University encourages the use of electronic communications to improve its effectiveness, but users need to:

a) Be clear in stating whether their views/opinions are personal when participating in such forums to avoid giving the impression that they are representative of the University unless they are authorised to do so.

a) Remember that all messaging is a form of communication, which is subject to the general law on contract, copyright, defamation, etc. Therefore, always use the same discretion, courtesy, and consideration as any form of written communication. A University standard disclaimer should be used with all outgoing email.

b) Understand that electronic communications can be disclosed under a Freedom of Information or Data Protection Subject Access Request and care should be taken on its format and contents; proprietary information and sensitive or confidential material must have additional controls which can be requested via the University IT Service Desk.

c) Refrain from participating in the sending of unsolicited commercial or bulk email unless this has been authorised and is through the approved communications channels. Further information is available through the Communications & External Affairs Professional Service Unit.

Further information can be found in the University's Email Policy.

8. Internet and Electronic Trading

Information placed on the Internet becomes part of the public domain and the ability to patent it will be lost. Consequently, any confidential, proprietary, or potentially valuable information or data shall not be placed on the Internet including unauthorised cloud services.

Any user that uses the Internet to buy or enter into leases or licences, on behalf of the University, shall ensure that any services or goods are supplied on terms and conditions of business that are acceptable to the University. All Financial Manual requirements in respect of approval for commitments shall be adhered to, and in some cases, it will be necessary to ensure which law and legal system applies and the currency of the transaction. Wherever possible, the University's standard purchase order terms should apply when buying goods.

Approval from the Director of Finance is needed before any Web page is set up with the intention of facilitating the acceptance of online credit/debit card payments.

9. Unacceptable Use

All use of the Internet and computer network is subject to the Jisc Acceptable Use Policy and unacceptable use of the IT systems, services and facilities is defined as their use:

a) In contravention of legal requirements and University regulations

b) In a manner that causes interference with University academic and business activities

c) To upload, download or in any way transmit commercial software or other copyrighted materials belonging to third parties or the University (including articles, books, music or video clips), unless covered by a commercial agreement or the copyright owner has given their express permission or other such licence.

d) To intentionally create, download, access, store, or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. Should access to such material be required for academic or research purposes then permission should be gained from the relevant authority (i.e. Supervisor or Head of Group) and notified to the Director of Information Services.

e) To send defamatory, offensive, abusive, or threatening messages, or to needlessly annoy or cause anxiety to others, or to intentionally promote or provoke violent or criminal activities either within the university or to external parties.

f) For unauthorised personal commercial gain

Users should seek advice from Information Security (E. ITSecurity@cranfield.ac.uk) if they need to process UK Government 'classified materials'.

Users shall not construct, alter and/or forge the headers of email messages to fraudulently mislead other users or to prevent them from responding to messages.

NB. It is an offence under the Computer Misuse Act to access (or attempt to access) computer held data, or software, without the authority to do so. All users are provided with specific access permissions according to their role with the University and shall not abuse the position of trust that this accords them.

10. Computer and user account protection

a) All computers (including laptops) that connect to the University network shall run up-to-date security protection software. This software is designed to protect against known security threats.

b) Centrally managed devices have a number of security controls in place to protect users and information, and these must not be tampered with or disabled

c) Users shall not download a program or file from any untrusted source, including USB drives. If in doubt, contact the IT Service Desk.

d) All email links and attachments should be treated with caution as they are likely compromise vectors.

e) If you suspect that your computer or account has been compromised, stop using it and make a note of the symptoms before calling the appropriate IT Service Desk immediately.

11. Backups & Maintenance

To protect your data, you must always save your files to a network drive, as local drives are not backed up. All files on the central servers get backed up on a regular basis.

12. Enforcement of policy

The University has implemented safeguards against specific threats to ensure the availability and security of its IT systems and monitors and logs the use of its IT facilities for the purposes of:

a) Complying with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime, and ensuring national security (relevant legislation includes the Computer Misuse Act and the Counter-Terrorism and Security Act);

b) Detecting, investigating, or preventing misuse of the facilities or breaches of the University's regulations;

c) Monitoring the effective function of the facilities.

The University does not routinely monitor or filter access to external information, but will act upon concerns or intelligence (from internal or external agencies) to instigate monitoring of an individual's access to IT systems and their activities with or without their consent in order to establish whether there is any misuse or abuse of University IT systems and/or a breach of this policy.

Any suspected breaches in this policy will be investigated and information will then be passed to the appropriate management, Human Resources function or Academic Registrar within the University. Temporary disconnection and removal of any material found to be in contravention of copyright and other applicable laws may be immediately applied on the authority of the Director of IT or other relevant party. The University may then decide to take formal action against you, which in severe cases, could result in your dismissal or termination of studies. In addition, the University may be required to report the breach to law enforcement, or other appropriate bodies, and civil or criminal actions may follow.