Information Technology users’ policy and procedures

Information Technology (IT)

Please read and follow this policy carefully as it aims to protect you and your use of IT systems and services, and the confidentiality, integrity and availability of information processed, stored, and transmitted by them.

It is vitally important that everyone understands and has a collective responsibility for protecting data entrusted to us.

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 IT Service Desk.

Not following this Policy, could have potentially serious consequences for you and the University:

- We could be subject to embarrassment, loss of reputation, and/or regulatory action
- We may lose contracts, research, or commercial opportunities
- You may compromise the integrity and security of data, and/or IT systems and services (resulting in potential damaging impact on colleagues, students, customers or even your own personal data)
- You may be subject to University disciplinary procedures and/or break the law, which could result in civil or criminal proceedings

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

Thank you

Professor Karen Holford	David Ford
Chief Executive & Vice-Chancellor	Director of Information Technology

Scope

All IT users (e.g., staff, students, contractors) are subject to this policy irrespective of which devices they use to access IT resources, or the services used.

1. Purchase, installation, maintenance, and disposal of IT equipment

The University makes a significant investment in computer hardware to provide reliable and secure access to IT services. University hardware must be purchased through IT Services (IT) and any installation, maintenance, relocation or ultimately disposal of IT equipment can only be undertaken by a representative of IT or through an approved IT Service Desk request. This applies to all PC’s, printers, computer cabling (although not applicable to device cable to wall socket) and associated University computer equipment. If alternative arrangements are required, then these should be discussed with the Director of Information Technology or nominee.

These measures mean that all University provided assets will be tagged, recorded centrally, appropriately configured and can be easily located for technical support to facilitate any proposed upgrades, etc. In addition, it will also ensure compliance with audit requirements and that the correct disposal procedures are followed.

Mobile devices (including laptops, tablets, and smartphones) will be subject to the requirements listed in 4.3.

2. Purchase, installation, maintenance, and disposal of software

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

- Users shall not illegally copy any software application used in the University, whether for business or personal use.
- Users should not retain any original software unless agreed once a licence is terminated.

Audits will be undertaken to reconcile commercial software use against licences, including restrictions on the number of users, and the ability to copy the software. All software must be updated in-line with the suppliers’ recommendations.

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

3.1 Personal data

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 several 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

Please note that you are responsible for any personal data (including recordings) that you store in emails, OneDrive, SharePoint or other Filestore, Teams and Zoom, and you must ensure that the data is secure (not shared with anyone who does not need access) using the tools provided and deleted when it is no longer needed.

For general advice on data protection matters email gdpr@cranfield.ac.uk.

3.2 Payment card information

The processing of credit card transactions is regulated by the PCI DSS (Payment Card Industry Data Security Standards) requirements on all organisations in the UK. For Cranfield, card details for processing a payment may come from the following sources:

- Payment online though WPM and Worldpay
- direct contact made by customer when invoiced, etc

All payments to be accepted online must be set up by the Finance Systems Team and will utilise the University’s third-party WPM and World Pay connectivity. This ensures that no credit or debit card details are held on any Cranfield University system that needs to be regulated under the PCI DSS regulations.

Further details can be found in the Credit Card Payment PCI DSS policy.

3.3 Data classification

The University has a formal classification policy, and all information will either be categorised as:

- Open; Information intended for public use and identifiable by context (being published in Journals, on the University website, or press releases etc).
- Internal Business; Data used for day-to-day business and academic operations by staff, students and University stakeholders not included in Confidential or UK Government categories.
- Confidential (Commercial or Personal Data); Information that if lost or compromised would have a significant adverse impact on the University or individual staff, students, or other stakeholders of the University. It should be noted that any bulk transfer of confidential data to third parties needs to be approved prior to release.

- UK Government (OFFICIAL or OFFICIAL-SENSITIVE); Most of the information that is created or processed by the public sector. 'Sensitive' is a handling caveat for a small subset of information marked OFFICIAL that require special handling by users.

Where there is a requirement for users to process UK Government ‘classified materials’ i.e., OFFICIAL-SENSITIVE (O-S) this can only take place in purposefully built ‘secure environments’; All such processing will be subject to Security Operating Procedures (SyOPs). No ‘classified materials’ above O-S can be stored on any part of the University IT network. If a user has a requirement to process ‘classified materials’, they must seek advice from the Information Security Team (E. ITSecurity@cranfield.ac.uk).

3.4 Intellectual property rights

To effectively manage the Intellectual Property (IP) that is developed at Cranfield, there is a need to identify IP that might be commercially valuable and to work with researchers to protect and exploit it. If you think that you have developed technology that can be commercialized, you should contact the Research and Innovation Office for guidance and support.

The University's IP Policy defines the main principles of IP ownership and responsibilities, and describes how commercially valuable IP is managed, protected, and exploited. It also includes a revenue sharing mechanism that determines how directly generated IP income can be shared between the staff inventors, and within Cranfield.

3.5 Backups and maintenance

To protect your data, you must always save your files to a network drive, as local drives are not backed up. Any data created in the ‘Secure Environment’ must only be backed up to the designated storage solution. All files on centrally maintained services get backed up on a regular basis – re. Data Back-up Policy.

All personal data held will be subject to Cranfield University's Retention Schedule.

4. Authorised use of IT equipment and services

4.1 Connecting to the Cranfield campus network

All IT equipment that connects to the IT network must meet the following conditions[1]:

- Run anti-malware software that is regularly updated from a central or supplier-based system
- Run a supported operating system that is regularly updated and patched
- Run applications that are regularly updated and patched
- The device has, where applicable (e.g. home PC), a software firewall
- Have an Internet Protocol (IP) address supplied through a Dynamic Host Configuration Protocol (DHCP) reservation[2], unless otherwise agreed with the IT Service Desk
- Have valid licence agreement(s) for any installed software

Server operating systems and software must not be operated unless their use have been agreed with the IT Service Desk.

[1] This will automatically apply where the equipment has been provided by and is managed by the University’s IT department.

[2] Means of joining an IT network

Network switches, routers, or other network equipment shall not be connected to the network or operated in a standalone mode, in the case of wireless network equipment, without prior consultation with IT Services.

In the event of a system interfering with normal network operations, or where it is exhibiting unusual traffic flows or activities then:

- The specific system/equipment will be disconnected from the network, or
- The network segment or subnet, local to the offending system/equipment, will be disconnected from the network, and/or
- The registered owner of the system/equipment will be blocked from using University IT services

Restoration of services will only take place once resolution of the incident has occurred.

Users based at Shrivenham will connect through the Serco provided DA_Guest network and will be subject to the terms and conditions of that network.

4.2 Access to data

All Cranfield University users will have unique login credentials, created automatically when users were authorised to use University IT resources, which must be used to access IT systems and services. Dependent on the type and level of access to data end user devices will need to meet security compliance controls before access is permitted.

These user accounts, based on a user account name and password, are created with Role-based Access Controls (RBAC) that are individually assigned to provide the appropriate level of access to systems and must not be shared or provided to other users. Therefore, if you change roles or move to a different team within the University you should contact the IT Service Desk to ensure that your access permissions are still appropriate.

Cranfield University staff, where authorised through the Access to Electronic Information process, may access files and communications, including email, stored on any IT facilities owned, managed, or maintained by Cranfield University and may examine the content and relevant traffic data. In circumstances where the University acts solely as a service provider for another body different rules may apply, contact IT for further guidance.

Any property of the University must be promptly returned when no longer required or as part of the leaving process

Multi-Factor Authentication (MFA) must be enabled on all accounts.

4.3 Mobile devices

Any mobile device, including personal, that accesses University data and IT systems must meet the following conditions (these are in addition to those for 4.1 and 4.2 above):

- Devices must be enrolled and registered with the University
- Devices must enforce some form of access controls (6-digit PIN, password, biometric, etc.)
- Devices must enforce an automatic lock on idle (no more than 10 minutes) or be locked manually if the feature is unavailable
- Devices must not have been jailbroken/rooted[3] i.e., maintains the integrity of the original operating system

[3] A device that has had the manufacturer's native operating system modified and therefore may be considered untrusted

- Devices must not be left unattended and unsecured where there is a risk of theft or unauthorised access
- Whilst the device is connected to the University network it must not be used to access, download, or store material that is in contravention of this (IT user's) policy – See Section 5
- Use of the device must not contravene any applicable legislation
- Cranfield owned devices are only to be used by the registered University owner
- When used on a home network ensure the network itself is secure

4.4 Cloud services

The University provides a range of Microsoft products (MS 365, SharePoint, Azure, and OneDrive) through enterprise agreements that offer cost-effective solutions for sharing and storing University data. These approved services ensure that the University can govern where data is held and apply appropriate security controls and conditions of use. This enables the University to provide applicable assurance statements to customers, partners, and other stakeholders that it meets legal and contractual conditions.

Therefore, whenever you have a requirement for procuring/using additional cloud-based services you must contact the IT Service Desk, in the first instance, who will be able to provide the appropriate advice, guidance and support.

There will always be a need to undertake a third-party supplier assessment prior to the use of any non-University provided services.

4.5 Personal devices

To meet the University's ongoing requirement to hold Cyber Essentials (CE) certification and meet external contractual obligations it must be noted that any personal device, that accesses University IT services and systems, will be subject to the following:

- Where required the user must allow IT to install an agent on any desktop/laptop (this will be used exclusively for the period of any CE assessment to demonstrate that the device meets the CE requirements)
- The desktop/laptop must have a non-Admin account installed
- The desktop/laptop must have anti-malware software installed which is regularly updated
- Any software installed on the desktop/laptop must be supported/licenced and be regularly updated
- Where required the security configurations and settings of smartphones and tablets will be provided to the assessor

In addition, the users of such devices must be available to support the CE assessment if their device is selected to be part of the CE sample.

5. Acceptable use of IT equipment and services

5.1 Acceptable Use

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

- In contravention of legal requirements and University regulations
- In a manner that causes interference with university academic and business activities
- 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.

- 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 Technology.
- To send defamatory, offensive, abusive, or threatening messages, 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.

For unauthorised personal commercial gain.

5.1 Electronic communications/Internet

The University encourages the use of electronic communications to improve its effectiveness, but users need to understand that their actions may have consequences and should:

- Be clear in stating whether their views/opinions are personal when participating in social media forums to avoid giving the impression that they are representative of the University unless they are authorised to do so.
- Remember that all messaging is a form of communication, which is subject to the general law on contract, copyright, defamation, etc. Therefore, use the same discretion, courtesy, and consideration as any form of written communication. A University standard disclaimer should be used with all outgoing email.
- 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 personal data or confidential material must have additional controls which can be requested via the University IT Service Desk.
- Refrain from participating in the sending of unsolicited commercial or bulk email unless this has been authorised and is through the approved communications channels.

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.

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.

Where emails contain information of a contractual or legal nature, these need to be retained for the same number of years as those that apply to printed materials to meet statutory or contractual requirements. Staff must not attempt to auto-forward all email to a non-University account and technical controls have been implemented to prevent this.

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.

Users should also note that any information placed online (Internet, social media channels, etc,) becomes part of the public domain and the University will lose its ability to patent applicable research. Therefore, any confidential, proprietary, or potentially valuable information or data shall not be placed on the Internet inc. unauthorised cloud services.

5.2 Secure access

Do not 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’s Password Policy. Change your password immediately if you think someone else knows it, or a device has been lost or stolen that was previously used to access University data.

Do not 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.

5.3 Remote working

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) 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, if possible, and avoid off-line working i.e., using the local device storage.

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

5.4 Personal use

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.

5.5 Incident reporting

All users need to contact the IT Service Desk as soon as practically possible if:

- You lose a device (including personal) that has been used to access University information
- You experience an issue with IT equipment
- You have found (or suspect) a fault or weakness in an IT system
- You are concerned about the contents of an email or believe it contains a malicious link or attachment
- If you believe that confidential, payment card or intellectual property information is at risk of loss or compromise

W: service.desk.cranfield.ac.uk
E: servicedesk@cranfield.ac.uk
T: 01234 754199

Opening hours: Monday to Friday 8.00am - 6.00pm.

If you lose or incorrectly transmit personal information, please report it to gdpr@cranfield.ac.uk immediately.

6 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:

- 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).
- Detecting, investigating, or preventing misuse of the facilities or breaches of the University's regulations.
- Monitoring the effective function of the facilities.

The University may monitor or filter access to external information on the basis of concerns or intelligence from internal or external agencies, or for safeguarding or other relevant reasons. Such monitoring of an individual's access to IT systems and their activities will be undertaken with or without their consent 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 Information Technology 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.

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.

Document control

Document title	Information Technology (IT) users' policy
Document number	CU-IT-POL-1.01
Originator name/document owner	Information Security
Professional Service Unit/Department	Information Technology
Implementation/effective date	February 2011
Approval by and date	Information Assurance Committee; 25/09/2023
Date of last review and version number	September 2023; V2
Date of next review	August 2024
Standards reference	Not applicable
Information categorisation	Open

Document Review

Version	Amendment	By	Date
2.0	Addition of Section 4.5 to cover personal device usage and requirements under the Cyber Essentials certification process. Re-wording of paragraph 3 (Section 6) to provide clarity on when filtering may be applied.	Information Security	September 2023