



# Acceptable Use Policy for External Partners

## Information Technology (IT)

This document applies to any external partner or contractor registered to use IT systems provided by Cranfield University and outlines the acceptable use of these systems.

## Introduction

The Janet network provides the University's IT systems to support the university's teaching, learning, research, and administrative functions. Jisc, who manage the Janet network, specify how these services shall be used under their Acceptable Use Policy, details of which can be found at:

<https://community.jisc.ac.uk/library/acceptable-use-policy>

## Use of University services

In summary, the University services should not be used:

- In contravention of legal requirements
- In a manner that causes interference with academic and business activities
- For the creation or transmission of material that infringes the copyright of another person or institution
- To intentionally access, store or transmit material which may be deemed offensive, indecent or obscene
- To send defamatory, offensive, abusive, or threatening messages
- To store classified material that has been designated for secure networks only
- To introduce viruses or other components of malicious software

## User actions & responsibilities

To take reasonable measures to satisfy these conditions all users should:

- Take appropriate steps to protect computing equipment from viruses and other forms of malicious software
- Ensure that the computing equipment is running a supported operating system that is regularly updated and patched
- Safeguard their password and change it if they believe it has been compromised
- Where available ensure all accounts are protected by multi-factor authentication
- Employ a PIN/password/biometric access method on any mobile device used to access the information
- Report any vulnerabilities or weaknesses found
- Assist in the investigation of any alleged breach of these terms and conditions

All IT Users must read and adhere to the University's IT users' policy - [Link](#)

## Monitoring & support

Be aware that network traffic may be monitored to aid network troubleshooting and problem resolution, and the University reserves the right to access all information stored and processed on its IT systems to ensure compliance with Janet network provisioning, University policies and all applicable legislation.

Further information or advice can be obtained by contacting the IT Service Desk –  
**W:** [servicedesk.cranfield.ac.uk](https://servicedesk.cranfield.ac.uk); **T:** 01234 754199; **E:** [servicedesk@cranfield.ac.uk](mailto:servicedesk@cranfield.ac.uk) or the University's Information Security Team – **E:** [ITSecurity@cranfield.ac.uk](mailto:ITSecurity@cranfield.ac.uk)

## Document control

<b>Document title</b>	Acceptable use policy for external partners
<b>Document number</b>	CU-IT-POL-6.01
<b>Originator name/document owner</b>	Information Security
<b>Professional Service Unit/Department</b>	Information Services
<b>Approval by and date</b>	Information Assurance Committee; 06/05/2025
<b>Date of last review and version number</b>	May 2025; V2.0
<b>Date of next review</b>	May 2026
<b>Information categorisation</b>	Open

## Document Review

<b>Version</b>	<b>Amendment</b>	<b>By</b>	<b>Date</b>
2.0	Addition of MFA and biometric access controls	Information Security	May 2025