AT A GLANCE: INFORMATION SERVICES ACCEPTABLE USE POLICY

Secure, fair, and legal use of information services

Aims

The main aim of this Policy is to help protect the University and its people from cybercrime. It sets out how everyone who uses University information services – University and College staff, students, and other users – can help prevent security-related incidents and avoid harmful activities.

By doing so, the Policy aims to reduce the following related risks for our staff, students and institution:

- Distress and increased vulnerability to fraud for staff, students, research participants or others if their personal data held by the University is leaked, lost or stolen.
- Lost productivity and disruption to work and study resulting from any service downtime, which could be especially damaging at business-critical times such as admissions or examinations.
- Increasing difficulty for academic staff applying for research funding as funders steadily increase cyber security requirements (e.g. UKRI 'trusted research' programme).
- Regulatory intervention and significant legal and financial penalties resulting from any data leakage, diverting resources from research and education.
- Reputational damage to staff, students and the institution resulting from successful attacks.

Finally, the Policy helps the University meet the requirements of its regulators, auditors, and insurers, which are evolving as cyber threats grow; and helps staff and students to obey relevant laws in their use of information services, such as the Data Protection Act and the Computer Misuse Act.

Headlines

Secure login

Don't share or re-use your password; follow guidance on choosing a strong password; enable multi-factor authentication if available; don't let anyone else sign in as you and don't sign in as anyone else.

Cyber security

Complete awareness training; run anti-virus software; and install updates promptly. Check that you can trust unexpected communications and any links, downloads, and devices that you access.

Data confidentiality

Safeguard the University's personal and other confidential or sensitive data: lock your screen when you leave your computer; and don't use a non-University email account to send such data. Use encrypted devices to store such data and secure or delete data on them before repair, disposal, return, or re-use.

Avoiding harmful activities

Don't do anything that may be illegal, that could deliberately or recklessly undermine security, or that could interfere with other users' work, rights, or legitimate use of services. Follow University policies.

Personal use

Personal use is allowed so long as it doesn't interfere with your work or others' use of information services. Your personal use must also adhere to University policies.

Report

Report incidents or suspected incidents as a matter of urgency. For a compromised password, malware infection, or security weakness, report to your IT support (see procedure). If a personal data breach is involved, also report via your local mechanism or to the Information Compliance Office (see procedure).

Information Services Acceptable Use Policy

A. Policy statement

1. People are at the heart of good cyber security. Everyone who uses the University's information services has a part to play in protecting them. This includes staff, students, and other users.

2. This Policy sets out what users must do to help prevent security-related incidents and avoid harmful activities. It also tells them how to report any suspected breaches so that IT staff can address weaknesses or minimize damage. It is impossible to protect against everything that may happen. However, using services in the right way can reduce the likelihood and impact of any incidents.

B. Scope

3. This Policy applies to everyone who uses the University's information services, including University and College staff and students and other users. It does not apply to guest and public users of the UniOfCam-Guest or eduroam wifi networks. See the definitions in Section C for more detail.

4. The Policy applies to all parts of the University. It also applies to users of University information services at Cambridge University Press & Assessment, University subsidiary companies, the Colleges, or any other entity. This includes any person accessing information services at entities connected to the University Data Network. Any such connected entities, including the Colleges, should therefore reference this Policy within the terms of use for their information services.

5. Some aspects of this Policy cover areas governed by law. Users must comply with the law, and should there be any conflict, complying with the law takes precedence over this Policy.

C. Definitions

6. For the purposes of this Policy:

    a. 'University' refers to the academic University and so 'University information services' to information services provided by any part of the academic University. The terms as used in the Policy do not include reference to Cambridge University Press & Assessment, University subsidiary companies, or the Colleges, or their separately provided information services. Users at these or any other entity are in scope only as far as they use University information services including the University Data Network (see Section B). For the avoidance of confusion between University-provided information services and the institution 'University Information Services (UIS)', the latter is referred to by the acronym 'UIS' only in this Policy.

    b. 'information services' refers to all IT systems, networks, and equipment provided by the University including its constituent institutions. This covers, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, internet access including through UniOfCam Wi-Fi services, data and voice networks including the University Data Network, networked devices, software, electronically-stored data, portable data storage devices, cloud services, thin clients, third party networking services, video conferencing systems, telephone handsets, and all other similar items commonly understood as information services.

    c. 'use' covers all forms of use and access, and includes the use of personally-owned systems, networks, or equipment, such as users' own laptops, tablets, or smartphones, when these are connected to the University's wired or wireless (Wi-Fi) networks or accessing University data.

    d. 'user' refers to any person authorised to use the University's information services through issue of a unique identifier, with the exception of those authorised to use only the UniOfCam-Guest or eduroam wifi networks and no other services. Users as defined in this Policy may include staff, students, College staff using the University network, and any contractors or long-

term visitors who need access to fulfil their duties, among others. The UniOfCam-Guest wifi network provides access for short-term guests, short-term visitors, and members of the public.

e. a 'unique identifier' is a unique username or user ID that allows the University to identify the individual user of its information services and the user to log into the services. It may look like an email address.

f. 'data' means information in electronic form and 'University data' means data relating to University business or originating within or stored on University-owned or -managed systems.

g. 'personal data' means data that relates to an identified or identifiable individual. This is distinct from 'personal use' which is use for personal as opposed to University purposes.

D. Signing in securely and keeping sign-in details safe

7. Users must change any default password issued to them at first login. Users must not share their password with anyone, including University IT staff, for any reason.

8. Users must have a strong password for University information services and must not use the same password as the password they use for any services external to the University.

9. Users must store any record of their password securely, either by using a password manager or by keeping any written record safely, out of sight, and away from their devices.

10. Where available, users must set up two ways of confirming their identity on University systems. In addition to a password, ways of confirming identity include use of an authentication app on a phone or laptop, a one-time code sent to a phone, a call on a landline, or use of a UIS-provided token. Setting up alternative ways of confirming identity is known as multi-factor authentication or MFA.

11. Users must not log in with another user's account credentials; use logged-in services under another user's unique identifier; share their account credentials; allow a third party to use logged-in services under their unique identifier; or otherwise obtain or facilitate unauthorised access.

12. Where users have more than one account with different privileges, they must log into the account with the lowest level of access that allows them to perform the required task.

13. If any user suspects that their password may have been compromised, they must change it immediately and notify their local IT support or service desk. IT staff must follow the reporting procedure set out by the University's Computer Security Incident Response Team (CSIRT).

E. Protecting against malware

14. Users with an @cam or @<subdomain>.cam email address must complete University-approved cyber security awareness training annually.

15. Users must take reasonable precautions against the introduction of malware to University systems, including through personally-owned devices that connect to University networks. Reasonable precautions will be set out in UIS guidance and include but are not limited to:

    a. running up-to-date anti-virus software where possible and appropriate, which the University makes available to all users through the anti-virus software page on the UIS website;

    b. installing available security updates promptly, by enabling auto updates where possible, and in all cases within fourteen days of receiving notification of the update;

    c. verifying unexpected communications that ask for information, payment, or to log into a system, to ensure that they are legitimate (if in any doubt, users should look up a phone number from another source and call to check); and

d. only downloading data and using data storage devices from trustworthy sources and handing any unknown or found data storage devices over to IT staff.

16. Users must report any actual or suspected malware infection to their local IT support or service desk. IT staff must follow the reporting procedure set out by the University's Computer Security Incident Response Team (CSIRT).

F. Keeping data safe and confidential

17. Users must respect the security and confidentiality of all University and College data and especially personal or otherwise sensitive data. To support this, users must where possible:

    a. ensure that their computers and other devices used to access University information services are lockable with a password or pin and locked before being left unattended; and

    b. set their computers and other devices to lock automatically after at most ten minutes of inactivity.

18. Users must not use a private (i.e. non-@cam or -@<[sub-]domain>.cam) email account or private social media account to handle University or College personal or otherwise sensitive data.

19. Encrypting devices protects the data on them if they are lost or stolen. Users must:

    a. ensure that any laptops, tablets and smartphones that they use to store or access University or College data are protected by encryption; and

    b. encrypt any University personal or otherwise sensitive data saved on a USB stick or other portable data storage device, either by encrypting the files or by using an encrypted USB stick or device.

    For guidance and the phased introduction of this requirement, see Sections J and M below.

20. Users must ensure the security of all University data prior to disposing of computer equipment or sending equipment to third parties for repair or upgrade. Users must not provide their password or pin with the device. If the device is not encrypted, users must also first remove University data.

21. Prior to ending their relationship with the University, users must make appropriate arrangements for the secure return of all University devices and equipment and for the handover and/or secure destruction of University data in their possession, unless alternative arrangements are agreed beforehand with their primary institutional contact and approved by their institution.

22. Users must report any personal data breach or suspected personal data breach relating to University data immediately, either through their institutional reporting mechanism or directly to the Information Compliance Office. Users must abide by the University Data Protection Policy.

G. Avoiding activities that may be illegal, weaken security, or harm other users

23. University information services must not be used for any activity that may reasonably be regarded as unlawful or in breach of the regulations set out by the University's network provider (see the Janet Network Acceptable Use Policy). Noting that, in individual cases, the following contractual and/or statutory requirements must be carefully balanced with the right to freedom of speech and academic freedom, this includes but is not limited to:

    a. Creation, access, storage, or transmission of any obscene images or other material, or any data capable of being resolved into such images or material.

    b. Creation, access, storage, or transmission of any material which promotes terrorism or violent extremism, or which seeks to radicalise individuals to such causes.

c. Creation, access, storage, or transmission of material with the intent to cause needless annoyance, inconvenience, or anxiety, or defamatory material, taking the Dignity@Work Policy as the guide to applying these contractual requirements within the University.

d. Creation or transmission of any unsolicited advertising or promotional material to other users, save where that material is embedded within, or is otherwise part of, a service to which the user or their institution has chosen to subscribe or which forms part of institutional business.

e. Creation, access, storage, or transmission of material with the intent to defraud.

f. Creation, access, storage, or transmission of material that infringes copyright law.

g. Use of software or data for any purpose that breaches licensing agreements or terms of use.

For research and teaching exemptions, see Section I of this Policy.

24. Users must not undermine the security of the University's information services, either deliberately or through reckless behaviour with a reasonable likelihood of weakening security. This includes:

a. Deliberate creation, download, storage, installation, or transmission of any data or material that the user knows contains malware, or any deliberate action to circumvent any precautions taken or prescribed by University IT staff to prevent infection by malware.

b. Download, installation, or use of security programs or utilities that reveal or exploit security weaknesses, such as password cracking programs, packet sniffers or port scanners, unless as part of the responsibilities of University or College IT staff or equivalently qualified IT staff at any other entity connected to the University Data Network.

c. Failure to comply with a request from a member of University IT staff to install software updates or carry out other security-related activity; or to desist from any activity that has been deemed detrimental to the security or operation of the University's information services.

For exemptions for research or other work purposes, see Section I of this Policy.

25. Users must not undertake deliberate or reckless activities that with reasonable likelihood could interfere with other users' work, rights, or legitimate use of services. This includes corrupting or destroying other users' data; violating the privacy of other users; and overloading services such that this denies service to other users.

H. Personal use of information services

26. University information services, including computers, email addresses, and network access, are primarily provided for academic and administrative purposes related to work or study at the University or associated entities such as the Colleges. However, many students and staff live in property owned by the University or Colleges and connected to the University Data Network. They and others have reasonable need to use University information services for personal purposes.

27. Personal use is allowed so long as:

a. it does not interfere with a staff member's work nor the performance of any other user's duties in relation to the University;

b. it does not contravene any University policies, including but not limited to the University's HR and information security policies; and

c. it is not excessive in its use of resources and does not in any other way cause any damage or difficulty to computers or to networks.

28. Any data relating to personal use stored on University devices or data storage services is subject to the same monitoring, investigation, and policy and legal compliance as data relating to University business. Users should be aware that they will lose access to such data should their accounts be

suspended or terminated. For this reason, users are advised to store data related to personal use on non-University data storage and to maintain a non-University email account for personal use.

I. Exemptions

29. There may be good reasons why some users need to contravene aspects of the Policy.

30. Those whose research or teaching may mean a contravention of an aspect of this Policy must first seek written permission from their Head of Institution. Depending on the contravention, the user and/or Head of Institution may also wish to take advice from the relevant research ethics committee, Legal Services, the Information Compliance Office, or the Chief Information Security Officer (CISO). Heads of Institution must report exemptions annually to the CISO.

31. UIS will seek to make all reasonable adjustments in implementing this Policy. Should any user still be unable to fulfil Policy requirements due to their disability, they should request further appropriate adjustments or an exemption from the CISO or their designated deputy via the UIS service desk.

32. Users must submit any other exemption requests for work or other reasons to the CISO or their designated deputy via the UIS service desk.

J. Transition arrangements

33. In the first year after the implementation date of this Policy, i.e. to 1 April 2025, users will be expected but not required to comply. Paragraph 19 relating to encryption will remain an expectation until 1 April 2026 when it will become a requirement. This is to allow for effective communication of the Policy and related guidance as well as staggered provision of UIS support for users needing assistance to comply. Users should begin working towards compliance as soon as possible.

K. Compliance monitoring and enforcement

34. The University reserves the right to audit the use of its information services to ensure compliance with this Policy and identify cases of misuse that endanger the University's operations or data.

35. During the first three years (to 1 April 2027), the compliance focus will be on:

    a. UIS monitoring of cyber security awareness training uptake, sharing with institutions where requested, and continued use of automated reminder system for non-completers.

    b. UIS provision of a technical monitoring solution that provides high-level data on devices connected to the University Data Network, including the status of anti-virus protection, security updates, and disk encryption.

    c. UIS provision of communications, guidance, and support to enable compliance, based on the need areas identified by monitoring and engagement activities.

    d. Regular engagement activities with users, such as short surveys or annual focus groups, to check levels of awareness and efficacy of UIS-provided communications and training.

    e. UIS reporting to the ISC on Key Performance Indicators (KPIs) from the monitoring data, incident data, engagement activities, and the exemptions process.

    f. ISC review of the efficacy of compliance and enforcement measures and the introduction of further measures as justified by the reporting.

36. In the vast majority of cases, the approach to breaches will be to provide supportive guidance and educational material. However, users should be aware that consequences of a breach could include temporary or if necessary permanent removal of access to University information services.

37. Refusal to engage with the Policy and associated processes may, in the most serious cases, result in the initiation of disciplinary procedures: for staff, the staff disciplinary procedure; for students,

the student disciplinary procedure; and for any other user, review of relationship with the University with primary institutional contact and/or Head of Institution and (if appropriate) HR representative.

38. In the case of proven gross misconduct, consequences could include dismissal. Suspected illegal activity may be reported to the police or other law enforcement agency.

39. Normal systems monitoring does not involve IT staff reading the content of users' email or files. However, the Head of Institution (or an appropriate deputy) and Director of Human Resources may jointly authorise specific staff to access a user's data in certain exceptional circumstances. These may include: where a user is under formal investigation for serious breach of a University policy or under investigation by a law enforcement agency; where there are justifiable grounds for concern for the safety of any user; where there is essential business need and the user's permission cannot be sought; or in similarly justifiable circumstances. In such cases, the user will be informed.

L. Summary of responsibilities

40. **All staff**, **all students**, and **all other users of University information services** must adhere to the responsibilities and required behaviours set out in this Policy.

41. **Heads of Institution or their deputies (departmental administrators, operations managers, or equivalent)** are responsible for: communicating this Policy to staff, students, and other users within their institution; encouraging compliance with the requirements; and approving non-return of equipment or data (paragraph 21).

42. **Heads of Institution** are responsible approving exemptions on research or teaching grounds (paragraph 30). They are also jointly responsible, **with the Director of HR**, for authorising staff to access users' data in certain exceptional circumstances (paragraph 39).

43. **University IT staff** are responsible for reporting any security incidents by following the incident reporting procedure set out by the Computer Security Incident Response Team (CSIRT).

44. **The Chief Information Security Officer** is accountable for the implementation, monitoring, enforcement, and annual review of this Policy; and approves or reviews exemptions (Section J).

45. **The Information Services Committee** will review this Policy at least every three years, or sooner if needed, taking into consideration the latest guidance on best practice issued by relevant external bodies, and recommend any changes to the General Board and the University Council for approval.

M. Related guidance and contact for queries

46. For guidance[1] on how to comply with this Policy see:

- Choosing a strong password
- Using a password manager
- Installing anti-virus software
- Keeping your device up-to-date
- Avoiding phishing attacks
- Encrypting your laptop
- Encrypting your tablet and smartphone
- Encrypting files on a USB stick
- Securing data prior to equipment repair or disposal (see also the University electronic waste collection service, which wipes data as part of secure disposal)
- Reporting a security incident (for all users)

[1] [All guidance will be reviewed and expanded before the effective implementation date to ensure that it is clear, comprehensive, and accessible, and missing guidance will be completed.]

- Reporting a security incident (CSIRT procedure for IT staff)
- Reporting a breach of personal data

47. Users must adhere to other relevant institutional policies, procedures, and guidance in their use of information services, including but not limited to their institution's HR policies, data protection policies, policies relating to appropriate staff and student behaviour, and free speech principles.

48. Some parts of the University have policies, procedures, and guidance on the use of local information services. It is expected that local guidelines will be consistent with this overall policy. If differences arise, the more stringent security requirement will take precedence.

49. The Terms of Use of the UniOfCam-Guest Wi-Fi Network govern its use by institutions, guests, visitors, and members of the public. The Guest Network is not intended for those who are entitled to internet access via the University Data Network and so its terms do not overlap with this Policy.

50. The eduroam conditions of use govern its use at the University and elsewhere.

51. If you have any further queries relating to this policy, please contact servicedesk@uis.cam.ac.uk.

Effective date of this Policy (v1.0): 1 April 2024

Date of next review: 1 April 2025