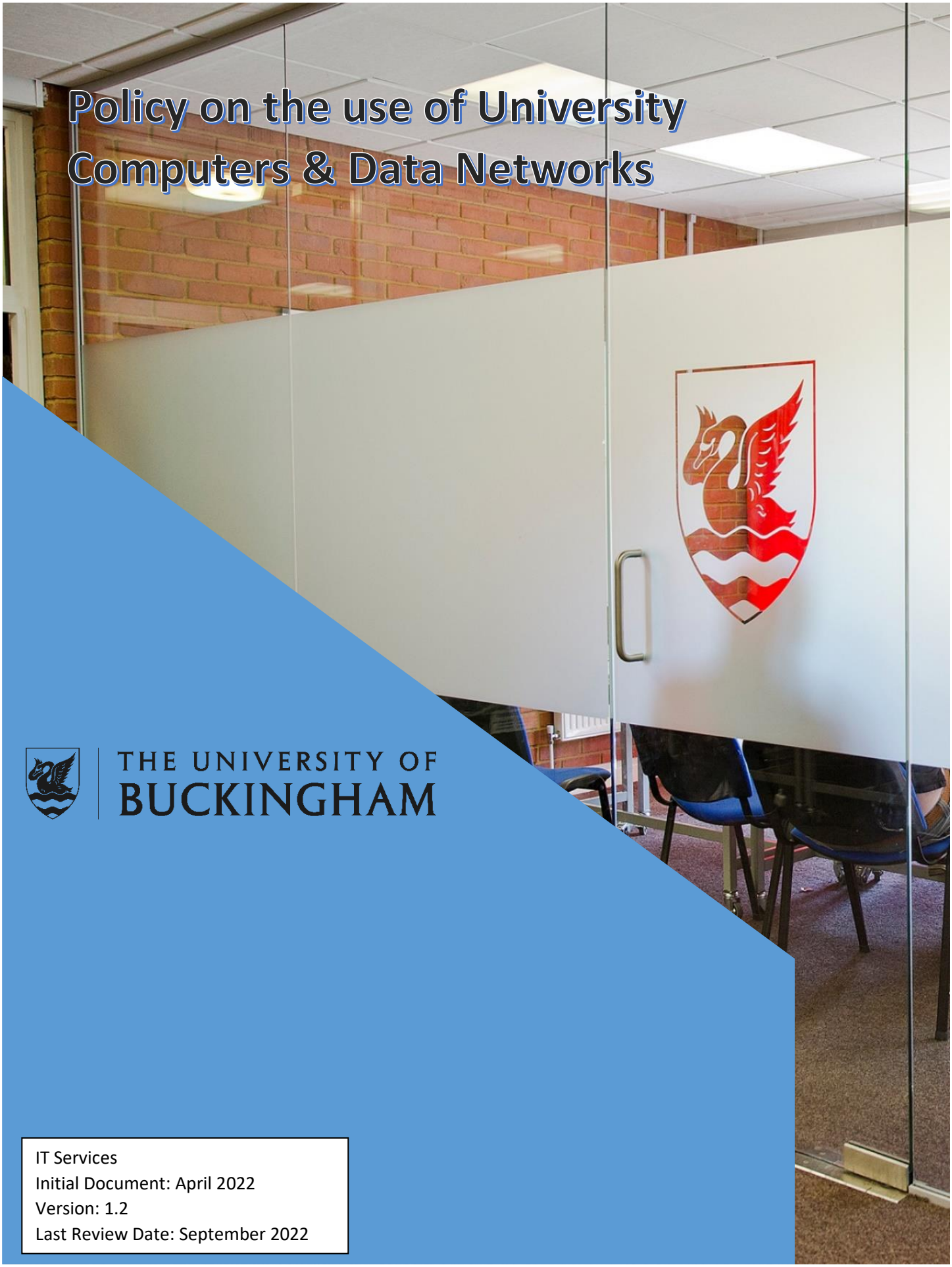
Policy on the use of University Computers & Data Networks



THE UNIVERSITY OF BUCKINGHAM

IT Services
Initial Document: April 2022
Version: 1.2
Last Review Date: September 2022

Table of Contents

1. Introduction

This policy covers the use of computers, data networks, and the associated services at the University of Buckingham. These facilities provide access to resources both on-and-off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

This policy applies to all members of staff and students of the University of Buckingham. Members of staff for the purposes of this policy includes, in so far as is relevant, employees, contractors, consultants, Trustees, independent members of the Council, examiners and invigilators, casual and zero-hour contract staff.

This policy covers the following:

a) The rules of using the systems – the "You Must" and "You Must Not".
b) How systems are implemented and managed.
c) The standards and guidelines to help you use the facilities in the best way possible.

This policy is intended to be an overarching standard for the myriad solutions in use within the University, and to remain extant through development and upgrades. Due to the fast pace of change associated with digital services it may be necessary to refer to additional procedures for specific services which are either published on the IT Hub or through the Knowledge Base articles on the Helpdesk portal. The Hub also contains guides and instructions should you require assistance due to a problem. If you can't find a solution to your query on those pages, then please contact the Helpdesk:

Online:	https://help.buckingham.ac.uk/sso/
Email:	helpdesk@buckingham.ac.uk
Telephone:	01280 820248

The Helpdesk is open from 09:00 – 17:00 weekdays and is the Single Point of Contact for all IT matters. All requests will be assigned a unique tracking number to provide audit and accountability before being logged to the most appropriate member of the department for action.

2. Applicable Legislation and Regulations

The IT operations of the University take place within a framework of primary legislation and regulatory requirements, and many of the rules that follow are in place to ensure compliance with these. It is therefore imperative that any development of IT systems is carried out with these requirements in mind and that implementation of new services or modification of existing does not cause a material breach. In addition, the University carries cyber insurance, and this may become void in the event that compliance is lost. This section is intended to give a non-exhaustive overview of the fundamental pieces and where further information is required the relevant University department such as Legal or Academic Services should be consulted.

2.1 Competition and Markets Authority (CMA)

Students have consumer rights, and the provided guidance outlines how consumer protection law applies to higher education providers.

2.2 Data Protection and GDPR

The University publishes a Data Protection Policy and Privacy Notice detailing how information is collected, stored, and processed.

2.3 PREVENT

The University complies with Section 26 (I) of The Counter-Terrorism and Security Act 2015 and publishes a PREVENT Policy detailing how IT systems and services are monitored and affected.

2.4 Regulation of Investigatory Powers Act 2000

The University complies with the terms of The Regulation of Investigatory Powers Act 2000. This Act makes it an offence to intentionally or without lawful authority, intercept communications without the express or implied consent of both the sender and the recipient of the communication. The Act allows for permitted exceptions to the principle that interception without consent is unlawful. These include measures to ensure the effective operation of the system, for instance:

- Scanning for viruses and other potentially harmful attachments.
- Monitoring email storage usage.
- Forwarding messages to the correct recipient.
- Eliminating spam.
- Investigating or detecting unauthorised use.
- Ascertaining compliance with regulatory practices or procedures. This must be authorised by the Legal Team and only in instances where there is reasonable suspicion of misuse.
- Preventing or detecting crime or in the interests of national security. This must be authorised by the Legal Team and only in instances where there is reasonable suspicion of criminal misuse or on the request of the police or specified public officials.
- Monitoring as per the PREVENT Policy.

The majority of the monitoring carried out by IT Services is done automatically and at the server level. There is no routine monitoring of email content by IT Services staff. For students, the data which records your access, and use of the University's systems may be used to improve your specific learning experience or used in a cumulative form to improve the learning experience in general at the University. This data will include your accesses and time spent on systems and hardware, assessment marks achieved and other relevant data.

2.5 Copyright

Users are required to respect the copyright of all materials and software made available by the University - the unauthorised copying or modification of software is an offence under the Copyright, Designs and Patents Act 1988. Further guidance on Copyright can be obtained from the Library.

2.5.1 Ownership of Material - Staff

The following paragraph is included in staff employment contracts as standard. Staff should refer to their own contracts in cases where this differs.

> Subject to any existing copyright in incorporated material and with the exception of any material that you have been requested by the University to produce for it, the copyright in any work produced by you in the normal course of your duties belongs to you.
>
> NB: Where any staff member is identifiable as the author of any material requested by the University, and where such material has been produced by you in the normal course of your duties, you shall, when requested by the University, do whatever may become necessary from time to time, including the execution of documents, to enable the University to exercise its rights over such copyright.

Lecture recordings are classed as a performance and therefore carry specific guidance.

2.5.2 Ownership of Material - Students

Copyright ordinarily belongs to the student, but all cases should be checked with the personal tutor for clarification. Research Students should additionally refer to section 7 of the Research Degrees Handbook for specific guidance.

2.6 Cyber Essentials

The University holds Cyber Essentials accreditation, audited and renewed annually. All systems are in scope, except for guest, residential and research networks. A number of University contracts depend on this accreditation being in place, and therefore measures must be taken to remain in compliance at all times. The requirements also extend to 3rd parties who require integration of their systems with our own, outside of the scope exceptions set above.

2.7 Payment Card Industry Data Security Standard

The University processes card holder data and therefore has an obligation to comply with the PCI DSS. These standards apply to all operations and external security tests are carried out quarterly.

3. Access to Services

3.1 Accounts

The University provides accounts and access to facilities to authorised users for the purposes of teaching, learning, research, administration, and approved business activities. Use of the University's account for personal purposes is permitted within reasonable levels, but for guidance, such use should not:

- Interfere with University responsibilities or with those of other University users.
- Jeopardise or interfere with the system so as to reduce the level of service for university business.
- Result in a negative impact on the University in any way.

Care should be taken when using a University account for personal use:

- Storing personal files, photos, and contacts may result in a breach of GDPR.
- University accounts are in scope for 'Subject Access Requests' and other forms of legal disclosure which could result in access being made to, or copies taken of, your personal data, or that of others.
- Signing up for subscription services such as Amazon or Netflix could be disrupted or lost.
- In all cases, access to the account will be lost when membership or employment ends and cannot be restored.

It is the University's policy and an audit requirement for Cyber Essentials to only provide users with individual, named accounts. Anonymous, generic, or shared accounts will not be provided, and where departments believe they have a requirement for such they should contact the Helpdesk who will examine the business case and suggest an alternative.

3.1.1 Staff Accounts

Accounts are automatically produced for staff as part of the employment process; they are therefore an HR function and IT Services do not create them. New starters will receive a document containing credentials either from their line manager or the HR department at the commencement of their contract. Access will not be provided in advance of the contract start date.

Accounts for honorary or associate members of staff follow the same process, subject to HR receiving the authorisation of the relevant Dean or of the Vice-chancellor and are subject to annual renewal. Former members of staff in receipt of this award will retain their email address but not their former mailbox.

3.1.2 Staff Access Levels

Staff access levels are determined by job classification and as an example, all staff receive a @buckingham.ac.uk email address but not all staff receive access to the PDR system. The entitlement matrix details the specific resources available. Many resources are purchased on the basis of staff status (such as FTE) and it would be a breach of conditions to falsify a classification in order to gain access. Staff will also receive access to other resources such as SharePoint libraries and shared drives depending on their specific department and role.

3.1.3 Staff Account Changes

The data for titles, names, job titles, job classification, department, and line manager are sourced from within the HR system. HR should therefore be notified of any changes that are required, and this will automatically update in linked systems. This process is designed to remove access to resources

associated with the prior role, in order to ensure compliance with GDPR and Cyber Essentials. Furthermore, when a member of staff takes on a new role at the university a new mailbox and home area/OneDrive will be provided, with the prior versions being retained for a period. If the staff member has a requirement to retain files and emails, this should be discussed and agreed with HR, and where necessary, Legal Services. It is for these reasons that we recommend departments make full use of shared facilities rather than retaining documents with specific staff.

3.1.4 Staff Account Closure

Staff accounts are disabled automatically at 18:00 on the final day of employment. Following two additional working days, the account and all data associated with it is deleted. Notification of leaving is the responsibility of the HR department, and line managers are responsible for the transfer of any data as part of the normal exit procedures. Line managers should ensure that University data is not transferred out of the organisation during these processes. Where exceptional circumstances require continued access for a discretionary period, a business case supported by the relevant Dean/Head of Department/Vice-Chancellor should be submitted to the HR Department for approval. HR will ensure that the time period and level of access meet our legal, compliance, and regulatory obligations, and will then arrange to extend the individuals contract as required. This extension should be noted in the Risk Register and monitored for closure.

3.2.1 Student Accounts

Accounts are automatically created for students as part of the registration process. Students will receive a notification of their account details via email.

3.2.2 Student Access Levels

Student access is standardised and all receive a Microsoft 365 A3 license, along with access to the online learning and library systems. Collaboration courses do not fall into this framework and will have bespoke arrangements. Additionally, some students may receive access to additional software dependent on their course of study.

3.2.3 Student Account Changes

Data comes from the student records system and changes are made by the Academic Services (Student Administration) department. Should a student change course or subsequently return for an additional, they will retain the same account if the separation between the courses isn't longer than our normal student closure procedures below.

Additionally, the Academic Services (Student Administration) department may request that access to a student account be curtailed or disabled in the case of disciplinary proceedings or other policy related matters.

3.2.4 Student Account Closure

Student accounts follow a closure timeline based on the date that the student complete their studies. Notification of leaving is the responsibility of Academic Services (Student Administration) department.

DOC + 7 days	the student's uCard expires.
DOC + 63 days	the student will receive an email reminder that their account will be disabled in 7 days, and that copies should be taken of any data required.
DOC + 70 days	the account is disabled.
DOC + 91 days	the account and all associated data is deleted.

3.2 Security

3.2.1 Password policy

Accounts are secured by the user with a personal password that is a minimum of 10 characters long. In keeping with modern security guidance, the University does not impose complexity rules nor mandate frequent changes, but instead recommends the NCSC guidance. The password chosen should be unique, and not used with any other service to reduce the chance of compromise.

Passwords must not be disclosed to any other party. In most cases IT Services do not require your password to provide technical support, but where this is unavoidable, a temporary should be set by you which is then reverted after the work has been carried out. If you are suspicious about a request to disclose your password, please contact the Helpdesk.

Account holders must not allow any other person access to their accounts even when the password is not disclosed, and care should be taken to either log off or lock your workstation when leaving your desk. For situations where access is required by another, such as a secretary accessing a manager's email account, see section 3.3.1. Sharing accounts undermines audit processes and compliance, and can result in serious consequences; as a result disciplinary action will be taken where this occurs.

3.2.2 Multi Factor Authentication (MFA)

Access to resources from off-campus requires the use of Multi-Factor Authentication (MFA) in addition to the use of a password. This process is compulsory and ensures that our users have an additional layer of protection in the event of an account compromise. Whilst the simplest method is the use of a mobile phone app, those that cannot or do not wish to use such can provide a telephone number (either personal or office) in order to carry out the required steps.

3.3 Data Storage

Staff and students are provided with an on-campus home drive, designated H:. Additionally, off-campus cloud storage is provided through Microsoft OneDrive. For collaborative working, shared drives are made available on-campus, and through Microsoft SharePoint. These areas are secure, encrypted, and audited. No data should be stored in any other location on the local disks of computers, laptops, or other devices. Under no circumstances should staff use portable media for the storage of data. Advice on sharing data can be found below or from the Helpdesk.

3.3.1 Accessing a colleague's data.

There are legitimate business cases where staff will need to be delegated access to the account of another member of staff. This generally occurs for personal assistants and can be facilitated by a request to the Helpdesk with approval from the individual concerned. The process provides a fully audited solution that protects all parties and does not require the sharing of credentials.

In cases of unexpected absence, a line manager alone can request access to an employee's email account and files for business purposes. Access will not be granted to team members at the same or lower level than the absent member of staff. This access must additionally be authorised by the Dean or Administrative Head of the Department, and wherever possible the user should be contacted to seek their permission. While permission is not required, managers should discuss any refusal with HR or Legal Services before proceeding.

3.3.2 Routine sharing

It is anticipated that during routine business there will be a requirement to share data with colleagues and external agencies. Before doing so, ensure that you are aware of the sensitivity of the data, and who the intended audience is. Do not share more than required and ensure that sharing will not cause a breach of GDPR, Copyright, or other elements of section 1. Guidance can be sought from IT Services or Legal Services.

IT Services recommends the use of OneDrive or SharePoint for sharing data. This ensures that the recipients are controlled, access is audited, and sharing can be withdrawn as required. The use of email is not recommended due to the lack of control and risk of interception. Further guidance is available on the IT Hub.

Platforms other than the above, such as Dropbox, FilesAnywhere, or WeTransfer must not be used for storing or transmitting University data. Should University members need to receive data through secure means, the LiFT Service is provided.

3.4 Privileged Access

3.4.1 IT Services

Members of IT Services necessarily require privileged levels of access to University systems. This access is provided through special accounts and capabilities vary based on the holder's position and responsibilities. Access is only used for legitimate reasons such as fault-finding and system maintenance, and all access is logged. Employees entrusted with privileged access are recorded in the IT Services Risk Register, and requirements will be reviewed on a quarterly basis.

In order to protect all parties, all requests for assistance must be routed through the Helpdesk to demonstrate a clear audit trail of requests, authorisations, and actions taken. Where circumstances require discretion, a holding ticket must be created by the requestor which contains the time stamp and location of the full request, preferably by email. Requests will not be actioned based on verbal instruction.

3.4.2 Legal Services

The Legal Services department are empowered to direct IT Services staff to carry out searches of data where this is required to fulfil their duties, and to take whatever means are necessary to comply with requests.

3.5 Supplier access

From time-to-time suppliers and support partners will require access to University systems in order to rectify faults, assist with upgrades, etc. Wherever possible this access will be facilitated through remote desktop services and a member of the department will monitor the actions taken. If this type of access is not suitable, a restricted user account will be created and only enabled as required.

4. Services

4.1 Email

All business correspondence must be carried out using a University email address – either the individual address allocated or via a shared or departmental mailbox. The automatic forwarding of all incoming emails to an external email address is prohibited. IT Services recommend that communications that could require retention are always sent from multi-user mailboxes to avoid emails being lost when staff leave or change roles.

Shared/Departmental mailboxes can be requested by any department and should be monitored by more than one person to avoid emails being missed during periods of absence. Requests should be made to the Helpdesk by the Dean or administrative head of department, detailing the requirement and the staff to delegate access to. Addresses should be requested with consideration to the whole organisation, and requests may be denied if there is a naming clash with another department's function that could lead to misrouted emails.

4.1.1 Email Transport and Management

Email is widely used as a method to attack organisations and there have been several instances in recent past where partner organisations have been comprised, subsequently putting the University at significant risk. Email security is therefore taken extremely seriously.

In order to prevent impersonation all email coming from a buckingham.ac.uk address must be sent from an authorised server. Authorisation is provided through technical means, and requests for new external services to use the University domain must be approved by the Head of IT. Servers that use our domain without authorisation will have their email rejected by the recipient. It should be noted that authorisation does not imply that the sender is safe, as responsibility for security rests with the external organisation and is out of IT Services' control.

As an additional protection against impersonation, the following banner is added to the top of all emails that originate outside of the University's email server – regardless of whether they have been authorised to send on our behalf or not. To avoid familiarity and complacence, IT Services will periodically change the colour scheme of the banner.

This email originated outside of the University of Buckingham. Unless you recognise the sender, and know the content is safe, do not click any links or open attachments. Please contact the IT Services Helpdesk if you have any concerns about the content of this email.

Incoming emails are passed through several stages of filtering and checking. At a global level the priority is to remove security threats and malware. Recipients of an email that has been quarantined will receive a notification, and the contents can be checked before release in the event of a false-positive. Whilst true spam is annoying, it does not represent a security risk and many such emails represent legitimate business-to-business correspondence. IT Services will therefore not routinely block incoming email unless it presents an ongoing threat to the organisation. The majority of low-level attacks will not repeat the sender address and blacklisting after the fact is futile. All users have the capability to manage their own mailboxes and choose who they do and do not wish to receive emails from – guidance is available on the IT Hub.

IT Services will not whitelist emails for any reason. Doing so removes all protections and puts the organisation at considerable risk. This is frequently requested by companies to account for their own poor security and misconfigurations and requests will be refused.

We ask users to be vigilant with all emails, regardless of sender, and to be especially cautious with attachments and links in messages. Always contact the Helpdesk with concerns.

If an email passes through the filters and threatens the integrity of the system, IT Services staff will use an automated process to delete it entirely from all recipients. Where an email is received that does not present a security threat, but nevertheless contains material that could cause distress (such as hate speech), authorisation will be sought from the Head of IT before any emails are removed.

4.2 Networks

The University uses a network segmentation model to isolate areas with different security needs. No devices should be connected to the network without the authorisation of IT Services, and the Helpdesk should be contacted should this be required, with particular reference to section 6. Connecting devices to the incorrect network can potentially cause a data breach.

4.2.1 Firewalls

Firewalls are used to control the flow of network traffic in and out of the University systems and are positioned at network boundaries. Because of the importance of the firewall requests for change are to be accompanied with a business case which will be reviewed for potential impact. Changes that affect networks rather than devices are to be approved by the Head of IT. A quarterly summary of changes will be presented to the Risk and Audit Committee.

4.2.2 Insecure Services

Some services are insecure by design and can be typically found in low-cost appliances such as network-enabled cameras and building management systems. Where the University has a requirement to use such, and the requirement cannot be reasonably avoided by using alternatives, then the solution must be risk assessed and the outcomes placed in the Risk Register. Authorisation to enable insecure services through the firewall must be signed off per section 4.2.1.

4.2.3 Web Filtering

All access to websites is monitored and matched against threat intelligence services and URL categorisation services to protect both the user and the University. In keeping with the principles of a modern, research focussed organisation, filtering is kept to a minimum. Blocked sites will typically contain content that is illegal under UK law, or would present a threat such as phishing and malware. Should a site be blocked incorrectly, please contact the Helpdesk who will review and submit the site for recategorization if required.

As part of the University's PREVENT policy, if a user tries to access to a website containing content classed as 'Weapons' or 'Extremism/Hate/Racism', the user will receive a message alerting the content, but allowing access once acknowledged. Access information for these sites will be logged and used as per the PREVENT policy. Students and supervisors are advised to make the Student Conduct team aware where material is being researched that could be captured under this policy.

4.3 Facilities

Access to buildings and some areas within buildings is controlled by individually issued uCards. These cards must not be shared and must only be issued to named individuals. Where generic cards are required for 3rd party access, e.g. contractors, the issue will be logged and controlled. Access to most rooms is controlled by keys. Requests for changes to access arrangements must be made to the Estates department.

4.4 Equipment

It is expected that equipment provided will be used responsibly and with due care.

Desktop computers must not be:

- Exposed to the risk of liquids or other substances.
- Moved. Requests to do so must be made to the Helpdesk.
- Altered in physical appearance, e.g., by stickers or writing.

Laptops and other portable devices must not be:

- Left unattended in an unlocked location.
- Left unattended in plain view, whether locked or unlocked.
- Exposed to the risk of liquids or other substances.
- Left in direct sunlight.
- Handled without due care.
- Lent to another person without authority of IT Services.
- Altered in physical appearance, e.g., by stickers or writing.

4.4.1 Damage to equipment

Equipment returned to IT Services will be checked for completeness and damage. In the event that damage is beyond reasonable wear and tear, or parts are missing, the issue will be reported to the Head of the relevant department. Replacement or repair will either occur from their own budget, or where there are grounds to suspect wilful or negligent damage, may escalate to Student Conduct or Human Resources as appropriate, who may charge you for repair.

4.4.2 Personal use

The University's IT facilities are for bona fide University activities. Permission must be sought from the Head of IT to use the facilities for commercial or outside work and such use may be subject to charge. Use of the facilities for personal work or recreation will only be permitted within reasonable levels and must not jeopardise or interfere with the system so as to reduce the level of service for university business.

4.5 Printing

The university runs a print management system to try to keep printing to essential items. All prints are monitored by the system. Student credits are renewed termly, and additional purchases can be made where required.

5. BYOD (Bring your own device)

Staff and students can use their own devices to access certain University systems using either the guest network on campus, or over the Internet. This access will be secured using MFA, per section 3.2.2. Installing applications such as Teams or Outlook on personal devices means that data can be accessed offline, introducing a security risk. As a result, the Microsoft Company Portal must be installed to provide a baseline of security compliance, such as ensuring encryption is enabled. The Company Portal also provides IT Services with the capability to wipe the device at the user's instruction in the event that it is lost or stolen, ensuring the security of data. Some users may prefer not to allow control of personal devices - the use of local applications is optional, and does not prevent users from accessing the web-enabled versions of these services which do not require the Company Portal.

IT Services cannot provide technical support for personal devices due to the myriad configurations possible and to protect both customer and department staff from issues that may arise from accessing personal data.

5.1 Processing University Data

Our Cyber Essentials accreditation requires that University data is processed on University-owned devices or software platforms. Staff needing to work from a personal device must therefore sign into the Staff Remote Access system before working with any data or use online software only.

When using a personal device, staff can:

- Use web-based versions of applications such as Teams, SharePoint, and Outlook
- Use the online editors for Word, Excel, and other documents
- Use the Staff Remote Access system for complete safety and security

When using a personal device, staff cannot:

- Download any University data

6. Requests for Change

6.1 New Projects

The University has many interconnected systems operating in a framework of competing requirements. In order to ensure that new solutions are fully interoperable and will not breach any regulations, IT Services must be involved at the outset of any new projects. Please contact the Helpdesk to raise a request. Customers may also find that a solution already exists which will avoid further expenditure – our service catalogue can be found on the IT Hub.

6.1.1 Purchasing and asset management.

In order to ensure best value for money and ongoing support, all purchasing for equipment and digital services should be made by IT Services. In the rare event that this is not possible, IT Services must be consulted before purchase to ensure that all necessary elements are included. We often find that warranties and ongoing software support is forgotten, which can lead to breaches in elements of section 1. IT services perform a yearly supplier review to work out the best supplier against cost and service delivered, with consideration given to the total cost of ownership including ongoing support requirements either from ourselves or external partners – the list price is only a small element of the eventual total. Our present specification for computer equipment is available on the IT Hub.

Assets purchased using University funds belong to the University and not to individual departments. IT services maintain the master asset record of equipment which informs the elements of section 1, and staff must not purchase and operate 'shadow IT'. To do so would cause a breach in compliance and could result in disciplinary action.

6.2 Requests for software

The University maintains a list of approved software that can be installed on our systems - Software List. Requests for additions to this list must be made in advance of requirement to the Helpdesk for review and testing. All software in use in the University must be correctly licensed and must be receiving updates through a support process. Free / Open-Source software is considered to be in support as long as updates are being released. Software is audited annually, and unused applications or applications that are no longer in support will be removed.

All software installations must be carried out by IT Services staff. Users are not permitted to install their own software even if it does not require administrator level access.

It should be recognised that IT Services are not experts in every piece of software, and even when software appears on the approved software list we may not be able to provide support for every issue that arises. Use of software outside of the approved list is permitted but at the users own risk.

6.3 Partnerships

It is expected that departments will enter formal partnerships with outside agencies and organisations. This may require data sharing, or the installation of equipment on our campus. Every new partnership must be formally risk assessed to ensure that all legal and compliance matters have been considered from the outset and are in place before proceeding. IT Services partners with bodies such as the NCSC and can provide specific threat intelligence on request – this is particularly relevant for research and working with foreign nationals. The outcomes should be stored in the Risk Register and reviewed annually.

Organisations operate to different frameworks of compliance, such as NIST, ISO27001, or Cyber Essentials. Where there is disparity between a potential partner and the University, the University's measures must be taken as the lowest level, and no reduction will take place to accommodate a 3rd party. This is especially important when operating across legal boundaries, and it must be ensured that partners in other nations are able to meet the minimum standards required by our systems.

7. Disclaimer of Liability

Whilst IT Services takes appropriate security measures to protect data and software, the University cannot and does not accept any responsibility for the loss of any data or software or the failure of any security or privacy mechanism.

The University accepts no responsibility for the financial or other consequences of the malfunctioning of any IT facility or part thereof, whether hardware, software or other.

No claim shall be made against the University, its employees or agents in respect of any loss, damage or inconvenience alleged to have been caused whether by defect in the resources or by act or neglect of the University, its employees or agents.

8. Failure to Observe the Rules

Failing to observe the rules laid out in this policy can result in serious consequences for the organisation and the individual. Loss of insurance, loss of accreditation, and loss of income can easily result from what may seem like trivial actions.

Any infringement of these rules constitutes a disciplinary offence and established disciplinary procedures will be followed for staff and students. In addition, infringement of these rules may be subject to penalties under civil or criminal law and the University is prepared to invoke such law. Authority is vested in the Head of IT and Officers of the University to temporarily suspend access to IT facilities by any user suspected of a breach of these rules pending full investigation.

For the general guidance of students, the least serious offences are liable to result in temporary withdrawal of facilities and a formal warning. More serious offences will carry longer terms of suspension and possibly fines, together with a formal warning. In the most serious offences termination of studies will be considered.