# IT Security Policy

## Contents



| Document Control Information | |
|---|---|
| **Version control** | **[1.0]** |
| **Owned by:** | **[ Director of IT Services ]** |
| **Latest amendment on:** | **[10/04/2022]** |
| **Approved by:** | **[ Senior Leadership Team]** |
| **Approved on:** | **[ 14 June 2022 ]** |
| **Coming into effect on:** | **[ 14 June 2022 ]** |
| **Review date:** | **[ June 2023 ]** |

# Introduction

## 1. Purpose

This policy ensures there are suitable measures in place to keep the University's networks, systems, people, and data secure. IT security is important in a knowledge-based organization where secure access to information is important to people, learning and teaching, research, administration, and management.

## 2. Scope

This policy applies to all staff and students using IT facilities owned by the University, including equipment, software, and services, employed by the University for business purposes. All members of the University (staff, students, and associates) together with any others who may have been granted permission to use the University's IT services, are subject to this and the Acceptable Use Policy.

## Definitions

### 1) IT Accounts

It is the University's policy to provide each staff, student or associate a unique IT account to access IT services, applications and equipment. The user must behave responsibly to ensure the integrity of their IT account, and the University will provide them with services such as a password management system and multiple ways to authenticate themselves to access university systems and data.

Where departments, units or business functions require shared access to accounts, the University's policy is to provide role-based access accounts which must have a named owner within the business unit that requires them and are subject to the same IT Security policies as individual IT accounts such as regular password changes and multi-factor authentication.

### 2) Personal Use of IT Facilities

University information and communication facilities, including email addresses and computers, are provided for academic and administrative purposes related to work or study at the University. Members of staff must not use a personal (non-University provided) email account to conduct University business.

University IT facilities may be used to access personal email accounts or store personal data, however all use of University IT facilities, including any personal use, is deemed to be subject to the University's Data Protection Policy found here: Data Protection Policy

## 3) Accessing University IT Services

To ensure University information and data remains secure University staff must use the IT equipment and software they have been provided with to connect to IT Services.

University staff are generally discouraged from using personally owned and managed equipment to access University IT services. Where personal mobile phones are used to access University systems, staff are encouraged to password protect their phones. However, if they do so their device must have an up-to-date operating system, disk encryption and an antivirus program; with access limited in scope or duration. Access to London Met data and IT services by staff using a personally managed device may be detected and revoked if it is found to be compromised or posing a security risk to other users or University services and data. Staff and students may connect personally owned and managed equipment to the University's wireless network; however, the University will disconnect personally owned equipment if it is found to be compromised or posing a security risk to other users or University services and data.

Further to reduce risk of data loss, members of staff and students should not connect any personally owned peripheral device which can store data (for example, a personally owned USB stick) to any University owned equipment, irrespective of where the equipment is located.

Unless encrypted, removeable USB sticks should not be used to store any sensitive or personal data.

All devices connected to the University network or owned by the University must be secured effectively by having:

- An up-to-date antivirus product.
- Storage encryption.
- Be set to receive automatic updates.

- A supported operating system that receives regular updates.
- Must not put at risk others by its use.

Devices found not to be secured effectively maybe disconnected from the University's network without notice.

**4) Unattended Equipment**

IT Equipment used to access University facilities must not be left unattended and unlocked. Members of staff and students must ensure that their computers are locked before being left unattended. Care should be taken to ensure that no restricted information is left on display on the computer when it is left unattended.

Care should be taken to ensure the physical security of all equipment when in transit and must never be left in an unattended vehicle. Please see the IT Equipment Policy for further information.

**5) Additional and Third-Party Compliance Requirements**

Listed below are security requirements the University and its user community must comply with to retain access to the internet, payment card services and software:

**5.1 JANET policies**

The University, along with other UK educational and research institutions, uses the 'JANET' (Joint Academic NETwork) electronic communications network and must therefore comply with JANET's Acceptable Use and Security Policies. Both policies are available from the JANET website.

**5.2 Payment Card Industry Data Security Standard** (PCI DSS)

The University must comply with the Payment Card Industry Data Security Standard (PCI DSS) when processing payment (credit/debit) cards.

**5.3 Software licence management**

All software used for university business must be appropriately licensed. The University must comply with the software and data licensing agreements it has

entered. During the negotiation process of such agreements, full consideration must be given to how compliance with the agreement can practically be achieved. Agreements may need to be specifically negotiated to enable the University to comply. Therefore, no software must be brought other than via Information and Technology Services. Further information can be found in the Software Policy.

### 5.4 Records management

The University is required to retain certain information, whether held in hard copy or electronically, for legally defined periods as stated in the Records Management Policy found here: Records Management Policy

## 6) Using Personally Owned Devices

Staff should not process or store University information on personally owned devices, in accordance with the Data Protection Policy.

## 7) Information on Desks, Screens and Printers

Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure.

Individuals handling confidential or sensitive information should be mindful of screen visibility so that they cannot be viewed by unauthorised persons and all computers should be locked while unattended. Screen privacy filters can be made available for this purpose.

## 8) Exchanges of Information

Whenever significant amounts of personal data or other confidential information are exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred, in

consultation with the University's Data Protection Officer. Regular exchanges must be covered by a formal written agreement with the third party in accordance with Outsourcing and Third-Party Compliance, which is included in the University's Data Protection Policy: Data Protection Policy

Information classified as strictly confidential may only be exchanged electronically both within the University and in exchanges with third parties if the information is strongly encrypted prior to exchange. Information classified as secret may not be transmitted electronically except with the explicit written permission of the information owner. Hard copies of information classified as strictly confidential or above must only be exchanged with third parties via secure (for example, special) delivery.

When exchanging information by email or collaborative systems such as Microsoft Teams, recipient addresses should be checked carefully prior to transmission.

Unsolicited emails, Microsoft Teams or Instant messages, telephone calls or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

University employees must not disclose nor copy any information classified as confidential or above unless they are authorised to do so.

## 9) Reporting Losses

All members of the University have a duty to report the loss, suspected loss or unauthorised disclosure of any University information asset to the information security team email: dsar@londonmet.ac.uk who as required will engage with the Legal Services team.

The following link provides important information regarding the Data Protection Policies and procedures including breach notifications: Data Protection Policies

## 10) User Management

### 10.1) Eligibility

User accounts will only be provided for:

- Permanent and fixed term university employees.
- Contractors and Temps
- Students
- Governors
- Emeritus staff and those who have otherwise been granted honorary or associate status (Associates will include staff from other organisations that provide services to the University and may require access to the University's information systems to fulfil their contractual obligations to the University. Associates may also include external research collaborators)
- Non-human (generic) accounts are subject to approval by the Director of Information and Technology Services and regular review

User accounts give users access to the network, and an email account. This user account then makes it possible for users to be given access to resources, information systems or facilities on an individual or group basis.

Visitors to the University including conference guests are permitted use the guest Wi-Fi.

### 10.2) Authorisation to Manage

The management of user accounts and privileges on the University's information systems is restricted to suitably trained and authorised members of the Information Technology and Services Department.

### 10.3) Account and Privilege Management

a) Accounts will only be issued to those who are eligible for an account and whose identity has been verified via the HR system or Student Information

System. The credentials for these accounts must not be shared to any other person, user or service.

b) When an account is created, a unique identifier (UserID) will be assigned to the individual user for his or her individual use. This UserID may not be assigned to any other person at any time (UserIDs will not be recycled).

c) On issue of account credentials, users must be informed of the requirement to comply with the University's Information Security policy and ITS Acceptable Use Policy.

d) Access rights granted to users will be restricted to the minimum required for them to fulfil their roles.

e) Procedures shall be established for all information systems to ensure that user's access rights are adjusted appropriately and in a timely manner to reflect any changes in a user's circumstances (e.g. when a member of staff changes their role or a member of staff or student leaves the University).

f) Privileged accounts are used for the administration of information systems and are distinct from user accounts. These accounts must only be used by system administrators when undertaking specific tasks which require special privileges. System administrators must use their user account at all other times.

**10.4) Creation of User Accounts**

a) User accounts can only be created from automated feeds from either the University HR or student records systems, there is no other way for user accounts to be created and, therefore, it is essential that University processes for the recruitment of staff and students are followed.

b) Temporary users, including agency staff and placements must be registered by a responsible sponsor using the affiliate registration and management system (ARMS), visiting students will only be given access if they are

registered in the student records system

c) Staff on Honorary contracts and Emeritus staff will all be recorded on the HR system.

d) User accounts for University Governors will all be requested by the University Secretary.

**10.5) Removal of User Accounts**

a. When staff or students leave the University their user accounts will have access to them deactivated.

**b.** After an agreed period, staff or students that have left the University and whose accounts have been deactivated, will be removed, according to the University's Records Management Policy: Records Management Policy

**c. Investigation of Computer Use**

The University respects the privacy and academic freedom of its staff and students and recognises that investigating the use of IT may be perceived as an invasion of privacy. The University may however, carry out lawful monitoring of its IT systems when there is sufficient justification to do so and when the monitoring has been authorised by the Vice Chancellor, Chief Operating Officer (or delegate) as recommended by Director of Information and Technology Services (or delegate).

Staff, students and other members should be aware that the University may access records of use of email, telephone and other electronic communications, whether stored or in transit. This is to comply with applicable laws and regulations, and to ensure appropriate use of the University's IT systems.

Decisions to access the IT accounts, communications and other data of members will be taken by the Vice Chancellor, Chief Operating Officer (or delegate) as recommended by Director of Information and Technology Services Director of Information and Technology Services (in conjunction with the Director of HR) to

ensure that such requests are free of bias and are not malicious. Investigations of this kind are sensitive and time-consuming.

### 11.1) The University's Powers to Access Communications

Only authorised University staff may access files and communications, including electronic mail files, stored on any IT facilities owned, managed or provided by the University and may examine the content of these files and any relevant traffic data.

The University may access files and communications for the following reasons:

- Ensure the operational effectiveness of its services (for example, the University may take measures to protect its systems from viruses and other threats).
- Establish the existence of facts relevant to the business of the institution (for example, where a case of suspected plagiarism is being investigated and there is sufficient evidence, the contents of an individual's communications and/or files may be examined without their consent with the authority of an authorised person).
- Investigate or detect unauthorised use of its systems.
- Ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the University's business.
- To access communications relevant to the business of the University for example, checking email accounts when staff are absent to access relevant communications).
- Compliance with information requests made under the Data Protection Act or Freedom of Information Act (individuals would in normal circumstances be notified).
- To prevent or detect Cyber Crime

Please see the procedure for the reporting of Information Security Incidents below.

## 11) Covert Monitoring

Covert monitoring of computer use will only be authorised in exceptional circumstances where there is reason to suspect criminal activity or a serious breach of University regulations and notification of the monitoring would be likely to prejudice the prevention or detection of that activity. The period and scope of the monitoring will be as narrow as possible to be able to investigate the alleged offence and the monitoring will cease as soon as the investigation is complete.

Only information gathered in relation to the alleged offence will be retained. This information will only be viewed by those for whom access is strictly necessary, for example in relation to potential disciplinary proceedings. Decisions to undertake such investigations will be made by the Chief Operating Officer after consultation with the Vice Chancellor, the Executive Director of People and the Head of the University Legal Services.

## 12) Passwords

Passwords are an important aspect of computer security and the failure to use strong passwords may lead to the compromise of information and information systems. The password policy applies to all users of IT Systems and has been implemented as a minimum standard for the creation of strong passwords to safeguard information, comply with external business requirements and adhere to best practice.

- Passwords must not be shared; this is a violation of University policy.
- When a password is changed, these are the minimum requirements (Some systems have more stringent requirements):
    - The account owner must create a password that is different from the last six passwords.
    - Passwords will expire after 180 days.
    - Password must be at least eight characters in length.

- Provisons of the policy:
    - All use of the London Metropolitan Universities account(s) is the responsibility of the person the account is assigned to.
    - Failure to conform to these requirements may lead to suspension of the account or other action as provided by University Policy or law.

Please see the Password Procedure and Guidance for Best Practices below for help to reset and change passwords.

### 13) Network and System Administration

The University's computer systems and networks must be managed by suitably skilled and qualified staff to oversee their day-to-day running and to ensure their on-going security (confidentiality, integrity, and availability). This is detailed in internal policies which set out the responsibilities and required behavior of those who manage computer systems on behalf of the University.

## Procedures

### Reporting Information Security Incidents

Requests for investigation under this policy may be made by any member of staff or student, although typically the request will come from a Head of Department or School. Occasionally requests are made from outside of the University, for example by the police. The request should be made to the Director of Information Technology and Services who will appoint an incident manager. Incidents involving a personal data breach will go to the Data Protection Officer to coordinate. Other security incidents should be reported to the Chief Operating Officer. Should this be considered a disciplinary matter any associated investigation would be in accordance with the relevant disciplinary policy / student regulations. Documented Policies, Procedures and Standards, plus education and training, will supplement these directives. Compliance with this Policy will be regularly monitored by the Internal Auditors.

Incident review requests should contain the following information:

- The name and department of the student or staff member whose computer or computing activity to be investigated.
- The reasons for the request.
- Where computer misuse is alleged, the evidence on which this is based.
- The nature of the information sought.
- Any other relevant information, for example, that the request relates to ongoing disciplinary or grievance procedure.

Actual or suspected security incidents, related to electronic information or systems, will be reported promptly to the Director of ITS or the Head of Operations,

Repeat or malicious requests in the opinion of the Director of HR and the Director of Information and Technology Services, will be reported to the Chief Operating Officer whom if they concur, it may be investigated in accordance with the relevant disciplinary procedure / student regulation.

**Password Procedure and Guidance**

**Password Best Practices**

- You should change your password from the default when you first use it. (On some systems, passwords for newly activated accounts will need to be changed at first use).
- You should change your password every 180 days if not prompted to do so by the system. (On most systems, your passwords will expire every 180 days. Passwords must be reset at first login after expiry).
- When you change your password, you should create a password that is different from the last six passwords and has not been used in the last 2 years.
- Your passwords should contain at least one alphabetic and

one numeric character. (Implemented on some systems).

- Use non-alphanumeric or special characters for optimum security (check whether all of your applications accept these characters).
- Don't use a common dictionary word, a name, a string of numbers and obvious passwords e.g. password, admin, blank, your User ID etc.

**Password Guidelines**

- New passwords should be significantly different from previous passwords.
- Passwords must not be the same as the user ID.
- Passwords should not include the first, middle, or last name of the user.
- Personal passwords should stored using a secure password management tool and not be written down, ITS can advise on secure password management tools for staff and student use.
- Passwords used for University accounts should not be used for non-University accounts (e.g. Hotmail).

**Password Support**

- After 10 incorrect password attempts an account will be locked for 15 minutes during which time no access to the account is allowed
- Staff or students enrolled in the password management service and have forgotten their password should go to: Password Manager Service and use the self-service facilities there.
- Staff or students not enrolled in the password management service and who have forgotten their password or need further assistance

should contact ITS through the IT Self Service Portal

- IT staff will never ask for a user's password. Do not disclose passwords to any IT staff including online chat agents and technicians on the out-of-hours telephone service, or anyone else, even if requested.
- There is a minimum of 5-day notice of impending expiry when logging in to University IT equipment.

**Annexes or Schedules**

Information Security Cybersecurity Responsibilities and Guidelines