

Information Security Policy

|  |  |
| --- | --- |
| **POLICY TITLE** | Information Security Policy |
| **DATE APPROVED** | 01 December 2021 |
| **APPROVING BODY** | Management Board |
| **VERSION** | 1.2 |
| **PREVIOUS REVIEW DATES** | N/A |
| **NEXT REVIEW DATE** | September 2024 |
| **OUTCOME OF EQUALITY IMPACT ASSESSMENT** | *No major change* |
| **RELATED POLICIES / PROCEDURES / GUIDANCE** | * IT Acceptable Use Policy
* Data Protection Policy
* Data Management and Governance Policy
* Risk Management Policy
 |
| **IMPLEMENTATION DATE** | Immediately following approval |
| **POLICY OWNER (JOB TITLE)** | Head of Information Services |
| **UNIT / SERVICE** | Library & Information Services |
| **CONTACT EMAIL** | helpdesk@cardiffmet.ac.uk |

# Version Control

|  |  |  |
| --- | --- | --- |
| **VERSION** | **DATE** | **REASON FOR CHANGE** |
| 1.0 | September 2021 | First version – updating and replacing the Electronic Communications Policy with an Information Security Policy and sub-policies (IT Acceptable Use and Data Protection) |
| 1.2 | 1.12.21 | Updated following feedback at Management Board on 1.12.21 |

# Introduction

## Information, in all its forms, is a primary asset of the University. Its effective curation and security are critical to maintaining and supporting the University’s operations, its financial viability and reputation. The Information Security Policy forms the keystone element of the University’s overall Information Security Policy Framework, which sets out the principles and roles and responsibilities that Cardiff Metropolitan University applies when meeting its legal responsibilities in relation to the security, protection, and governance of its information assets.

## It should be read in conjunction with the other policies and procedures that form part of that overall Framework. These are:

### *IT Acceptable Use Policy:* This Policy sets out the responsibilities and required behaviours of all users of IT facilities provided by Cardiff Metropolitan University

### *Data Management and Governance Policy:* This Policy describes the arrangements the University puts in place to assure the integrity and quality of data across all its systems

### *Data Protection Policy:* This Policy outlines how the University complies with the requirements of the UK General Data Protection Regulation (GDPR)

## All staff are expected to be aware of this policy framework and to comply with its provisions as is required by the Cardiff Met Code of Professional Conduct.

# Purpose

## The purpose of this Policy is to:

### Describe how the University’s information is safeguarded from both internal and external security threats that could have an adverse effect on its operations, financial position or reputation

### Outline the Universities responsibilities in relation to the information with which it has been entrusted

### Describe how the University protects the confidentiality, integrity and availability of information through the pragmatic use of controls to prevent, or reduce, undesired effects

### Ensure that all users of the University’s information understand their roles and responsibilities in relation to information security

### To provide an overarching framework for other relevant University policies.

# Scope

## This policy is applicable to:

### all individuals who have access to University information and technologies.

### all facilities, technologies and services that are used to process University information.

### all information processed, accessed, shared, manipulated, or stored (in any format) by the University in support of its operational activities, including the use of personal devices to carry out University business and to the use of any data held as a result of an individual’s role at the University

### internal and external processes used to process University information.

### all external parties that provide information processing services to the University.

## The policy will be communicated to all users of University information, and will be made available to relevant parties, as appropriate.

# Definitions

## *Staff* - Staff are salaried and non-salaried members of the University or contracted individually by the University to provide a service.

## *Student* - A person pursuing any course of study in the University.

## *Visitors* - A visitor is anyone, not a member of staff or student, requiring access to University premises or services.

## *Information* - The result of processing, manipulating, or organising data. Examples including but not limited to, text images, sounds, codes, computer programmes, software and databases.

## *Data* - Information in raw form.

## *Confidentiality* - Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

## *Integrity* - Property of accuracy and completeness.

## *Availability* - Property of being accessible and usable upon demand by an authorized entity.

## *Users* - Any individual, or group of individuals who access, process or view the University’s information.

## The terms ‘Information’ and ‘Data’ are used interchangeably within this document.

# Guiding Principles and University Commitments

## The University is committed to protecting the security of its information and information systems. It is also committed to a policy of education, training and awareness for information security .

## Information managed by the University shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information, and to ensure appropriate legal, regulatory and contractual compliance.

## To meet this intent, the University will undertake the following actions:

### prevent unauthorised disclosure, modification, removal, or destruction of information

### prevent unauthorised access to information systems and applications

### ensure that senior management provides sufficient direction and support for information security that is aligned to the University’s strategic objectives and relevant laws and regulations

### establish management frameworks to initiate and control the implementation and operation of information security within the University

### ensure that employees, students and contractors understand their responsibilities in relation to information security

### provide active management of information security risk through the University’s risk management frameworks, reporting to the Executive and the Board.

### limit access to information (need to know) and information processing facilities

### prevent unauthorised access to information systems and applications

### prevent unauthorised physical access, damage and interference to the University’s information and information processing facilities

### ensure proper and effective use of encryption to protect confidentiality, authenticity and/or integrity of information

### ensure the correct and secure operations of information processing facilities

### ensure that information and information processing facilities are protected against malware

### backup information to protect against the loss of data

### conduct logging and monitoring to detect anomalies and generate any evidence that may be required to support investigations

### Maintain and update operational software and applications to ensure the integrity of operational systems

### carry out technical vulnerability assessments on a regular basis

### ensure the protection of information in the University’s networks and its supporting information processing facilities in line with the Data Protection Policy

### maintain the security of information transferred within the University and with any external entity

### ensure that information security is an integral part of information systems throughout their lifecycle (from concept to disposal/termination)

### ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses, through the management reporting line, and to agencies and authorities as recommended by the university compliance officer, in accordance with the severity of the event or incident.

### embed information security into the University’s business continuity management systems

### ensure compliance with legal, statutory, regulatory or contractual obligations related to information security and any security requirements

### ensure that all users conduct mandatory information security and data protection awareness training

### ensure that this information security is implemented and operated in accordance with this policy and other, supporting, policies, procedures or standards.

# Roles and Responsibilities

## The following bodies and individuals have specific information security responsibilities:

### The *Policy Owner* has operational authority for the security of information within the University and develops policies that underpin the controls needed.

### The *Digital Strategy Committee* (DSC) has executive oversight for information security within the University. DSC has responsibility for overseeing the management of the information security risks to the University's staff and students, its infrastructure and its information.

### The *IT Security Team*, once created (anticipated for 21/22), will have a significant role in delivering and applying this policy, as well as establishing groups and roles to deliver key developments.

### The *Information Compliance Community of Practice* includes representation from each School and Unit. Its members are expected to act as champions for good information security and governance in their areas and to support, guide and help to develop best practice

### *Governors* will assure that the risk management processes surrounding Information Security is sufficiently robust and capable of protecting the organisation, its staff and students effectively.

### *Management Board* will provide final approval for policies, and an escalation point for issues.

### *Information Asset Owners* will ensure that the assets they represent operate securely.

### *Data Stewards* play a leading role in ensuring data robust governance, typically against a given system.

### *Users* are responsible for applying the guiding principles described here and the requirements outlined in detail in the IT Acceptable Use Policy. In particular:

* take reasonable steps to prevent unauthorised disclosure, modification, removal, or destruction of information
* be accountable for safeguarding their authentication information (e.g. passwords) and follow University authentication guidance
* prevent unauthorised access to information systems and applications
* report incidents of improper use of the University’s information that may constitute a breach of this policy or sub-policies
* ensure proper and effective use of encryption to protect confidentiality, authenticity and/or integrity of information when appropriate to do so
* take reasonable steps to prevent loss, damage, theft or compromise of assets and interruptions to the University’s operations
* ensure that their information processing facilities, e.g. mobile phones, computers, etc. are correctly maintained, patched and have up to date malware detection to enable secure operations
* ensure that they backup any information of value held on or accessed by their own devices, to protect against the loss of data.
* maintain the security of information used or transferred within the University and with any external entity
* ensure compliance with legal, statutory, regulatory or contractual obligations related to information security and any security requirements by following the provisions of this, and related, policies and guidance.

## The University will conduct information security compliance and assurance activities, facilitated by the University's IT Security Team, to ensure the requirements of the policy are met. Wilful and/or repeated failures to comply with the Policy will be treated seriously by the University and may result in enforcement action on a group and/or an individual, which may include, but is not limited to, investigation under the Staff or Student Disciplinary Procedure as appropriate.

## Further guidance is available by contacting the IT Helpdesk on 02920417000 or via email on ithelpdesk@cardiffmet.ac.uk.

# Related Policies and Procedures

## This Policy should be read in conjunction with the following University policies:

* Data Protection Policy
* IT Acceptable Use Policy
* Data Management and Governance Policy
* Freedom of Information Policy
* Records Management Policy
* Staff Disciplinary Policy
* Student Disciplinary Procedure.
* Risk Management Policy
* Cardiff Met Code of Professional Conduct

## Copies of these policies are available from: <https://www.cardiffmet.ac.uk/about/policyhub/Pages/default.aspx>

## In its application of this Policy, the University will ensure that it complies with all relevant UK legislation, including:

### UK General Data Protection Regulation (GDPR)

### Freedom of Information Act 2000

### Computer Misuse Act 1990

### Counter-Terrorism and Security Act 2015

# Review and Approval

## The policy will be reviewed and updated every three years unless legislative or statutory changes necessitate earlier review.

## The approval authority is the University’s Management Board.