

Ref: Policy Set for all staff and contracted 3rd parties
Creation date: 31.03.2017
Next Review date: 01.10.2017
Version: 1.5 Final



Information Security Policy Set – All OU Staff and Contracted Third Parties

This document is a collection of the OU Information Security Policies designed to govern the use of OU information assets

OU – Information Security Team

Information Classification: **Public**

Table of Contents

Policy Enforcement	3
Exception to policy.....	3
Policies that apply to you and how you use your computer	4
Information Acceptable Use Policy.....	4
Computer Acceptable Use Policy.....	6
E-mail & Instant Messaging Acceptable Use Policy	8
Internet Acceptable Use Policy.....	10
Password Policy.....	12
Policies that apply to your work	13
Information Classification Policy.....	13
Access Control Policy	15
Data Encryption Policy	17
Technical Controls.....	17
Media Disposal Policy	19
Information Security Exceptions Policy	20
Information Security Incidents Policy	21
Policies that apply to you when working outside the office.....	22
Mobile Device Policy.....	22
Remote Access Policy.....	23
Policies that apply to you if you work with third party suppliers	24
Third Party Services Security Engagement Policy	24
Policies that apply to you if you take card payments.....	26
Payment Card Policy	26

Policy Enforcement

Any breach of these policies is significant as it may undermine the effective running of the OU and its ability to meet its duties and legal obligations. Failure to comply may lead to disciplinary action, including dismissal for serious or repeated breaches. It may also be the case that your conduct and/or action(s) may be unlawful. The OU reserves the right to inform the appropriate authorities in such cases. You should note that you may be personally liable for actions and or conduct arising from the use of OU Systems.

Exception to policy

- 1.1 Exception to Information Security policies will be considered where there is a justified requirement and the additional risk and/ or cost to mitigate that risk can be balanced with the business benefit.
- 1.2 For an exception to be considered an Exception to security policy request form must be completed.
- 1.3 All exception requests will be considered and processed by IT Information Security.
- 1.4 Approved exception to policy requests will be logged and regularly reviewed.

Policies that apply to you and how you use your computer

Information Acceptable Use Policy

Purpose

This policy defines the acceptable use of Information in order to protect students, research participants, staff and other confidential information and the University's information systems.

Overview

The Information Acceptable Use Policy covers general secure practice for information handling and should be read in conjunction with the other Information Security policies.

It is the responsibility of every computer user to know and follow this policy.

Scope

All users of OU information and information systems.

Policy

1. Information security classification

- 1.1 Information Asset Owners are responsible for assigning the classification of their OU information so that appropriate controls can be applied (See Information Classification Policy).
- 1.2 Users must apply and abide by the controls defined within the appropriate Information Security specific policy when processing or storing this information.
- 1.3 Information assets assigned an information security classification must be marked with the information security classification.

2. Information storage and transmission

- 2.1 Unless otherwise approved by IT, information must be stored on Central University Storage, ensuring availability and effective secure storage.
- 2.2 When exchanging information with a third party, you must ensure that it is conveyed securely. Seek advice from the Information Security team and refer to the Third Party Engagement Policy if you are unsure how to do this or which standard needs to be followed.
- 2.3 Mass extractions of Highly Confidential information must be authorised by the Information Asset Owner.

3. Use of confidential information

- 3.1 Do not forward, send or disseminate information assigned an information classification in any way that may compromise the OU or its students. If in doubt speak to your line manager or the Information Asset Owner.

4. Data protection legislation

- 4.1 The University is subject to UK legislation including Data Protection and Freedom of Information legislation. It is therefore essential that you also adhere to the University's [Data Protection Code of Practice](#).

5. Information retention

- 5.1 The OU has an information retention schedule which lists types of records, and the length of time they should be retained based on business needs. The OU retention schedule can be found at the [Information Management site](#) within Library Services.

6. Monitoring and privacy

- 6.1 For security and maintenance purposes, authorised individuals within the OU central IT teams may monitor all information, systems and network traffic at any time to ensure compliance with this and other security policies, and the effective operation of the University's systems.

Computer Acceptable Use Policy

Purpose

This policy defines the acceptable use of OU computer equipment in order to protect the OU's information and systems from risks including information loss, viruses and hacking.

Overview

The Computer Acceptable Use Policy covers general secure practice for computing and mobile devices and should be read in conjunction with the other Information Security policies.

It is the responsibility of every user to know and follow this policy.

Scope

All users of OU information and information systems.

Policy

1. Accessing OU systems

Users are provided with a username and password to access OU IT services.

- 1.1 Do not disclose or share your username or password, and keep your authentication device secure.
- 1.2 Passwords must be changed regularly. See the Password Policy for more information.
- 1.3 Do not allow anyone else to use your username or password.

2. Ensuring information confidentiality

- 2.1 Computers and mobile devices must not be left unattended whilst unlocked.
- 2.2 Take extra care with computer equipment and information when working in a public place. For example, protect your password input - if sensitive information is on the screen, consider your working location, and do not leave your equipment unattended when travelling.

3. General use and privacy

- 3.1 For security and maintenance purposes, authorised individuals within the OU central IT teams may monitor any information, systems and network traffic at any time to ensure compliance with this and other security policies, and the effective operation of the University's systems.
- 3.2 Users of OU computing systems must abide by all applicable laws.
- 3.3 The OU is under a statutory duty to have regard to the need to prevent people being drawn into terrorism. Should the use of OU computer equipment, information and Systems, give rise to a concern that a person may be at risk, this will result in action being taken in accordance with the OU Prevent Strategy.
- 3.4 The theft or loss of any OU or personally owned IT equipment containing OU information must be reported to the IT Helpdesk.
- 3.5 Only mobile devices used in conjunction with IT-approved mobile device solutions and configurations, as described in the Mobile Device Standard, may be used to send or store classified information.

4. Protection from malware

- 4.1 All computers and mobile devices connected to OU networks must have the latest security updates installed and operate up-to-date antivirus software. Any exception to this must be agreed with the Head of IT Security.
- 4.2 Files shared, downloaded or received by email may contain malware. If you are in doubt about a file, do not open it and report the issue to the IT Helpdesk.

5. Personal use

- 5.1 Incidental and occasional personal use is permitted, subject to the restrictions contained in this policy. Personal use is allowed so long as the use does not interfere with official business, contravene any other OU policy, detrimentally affect other employees or systems, or harm the OU's reputation.
- 5.2 Subject to personal usage (see 5.1), systems must only be used to fulfil the requirements of your role at the University.

E-mail & Instant Messaging Acceptable Use Policy

Purpose

This policy defines the security policy for email and instant messaging in order to protect the OU's information and systems.

Overview

This policy covers general secure practice for email and instant messaging services and should be read in conjunction with the other Information Security policies.

Technical terms used within this document are defined in Appendix A. The terms email and instant messaging are used interchangeably in this document.

It is the responsibility of every email user to know and follow this policy.

Scope

All users of OU information and information systems.

Policy

1. Confidentiality

- 1.1 You must delete any emails received in error, which were intended for someone else.
- 1.2 Before you send a message, make sure the addressees are approved to receive the information contained in the email.

2. Use of messaging services

- 2.1 Care must be taken when using email, as all expressions of fact, intention and opinion via messaging could be held against you and/or the OU in the same way as verbal and written expressions.
- 2.2 Email is subject to release under the relevant sections of the Data Protection and Freedom of Information acts. Deleting emails after a request has been made is an offence.
- 2.3 Do not send messages that might affect or have the potential to affect the performance of the OU systems, network and/or third party in any way. If in doubt please speak to the IT Helpdesk.
- 2.4 The University may automatically block or quarantine any email identified as a potential threat to the organisation.
- 2.5 Personal email accounts must not be used to conduct official university business.
- 2.6 The OU is under a statutory duty to have regard to the need to prevent people being drawn into terrorism. Should the use of OU computer equipment, information and Systems, give rise to a concern that a person may be at risk, this will result in action being taken in accordance with the OU Prevent Strategy.

3. Unacceptable use

The following activities are prohibited:

- 3.1 Attempts to read other users' messages without their express permission.
- 3.2 Auto forwarding of OU emails to third party email services.

4. Unsolicited email or junk email

- 4.1 The OU understands that individuals cannot control or prevent some unsolicited emails; however, users must not encourage others to send them such emails.
- 4.2 Some junk emails can be offensive, contain links to inappropriate web sites or contain viruses. Most junk emails will be filtered, however if you do receive emails from untrusted senders, you should delete them.

5. Monitoring and privacy

- 5.1 For security and maintenance purposes, authorised individuals within the OU central IT teams may monitor any information, systems and network traffic at any time to ensure compliance with this and other security policies, and the effective operation of the University's systems.

6. General use and ownership

- 6.1 The OU provides an email and instant messaging service to support University activities, and access is granted to users on this basis. Messages sent or received on University systems form part of the administrative records of the OU.
- 6.2 Incidental and occasional personal use is permitted, subject to the restrictions contained in this policy. Personal use is allowed so long as the use does not interfere with official business, contravene any other OU policy, detrimentally affect other employees or systems, or harm the OU's reputation.

Internet Acceptable Use Policy

Purpose

This policy defines the acceptable use of OU internet facilities to protect the OU's information systems.

Overview

The Internet Acceptable Use Policy covers general secure practice for the use of OU-supplied internet facilities, and should be read in conjunction with the other IT security policies.

Technical terms used within this document are defined in Appendix A.

It is the responsibility of every computer and information user to know and follow this policy.

Scope

All users of OU information and information systems.

Policy

1. General principles

- 1.1 Use of the internet is permitted and encouraged to support the goals and objectives of the OU. The internet is to be used in a manner that is consistent with the OU's [Behaviours and Standards at Work Policy](#) available on the HR website.

2. Personal use

- 2.1 Incidental and occasional personal use is permitted, subject to the restrictions contained in this policy. Personal use is allowed so long as the use does not interfere with official business, contravene any other OU policy, detrimentally affect other employees or systems, or harm the OU's reputation.

3. Internet usage

The following activities are prohibited unless they are a specific requirement of your role:

- 1.1 Downloading any software or files without OU-approved virus protection measures.
- 1.2 Downloading any software unless your job specifically requires this and such downloads are fully licenced.
- 1.3 Visiting hacking sites or downloading hacking or evidence-eliminating software.
- 1.4 Intentionally visiting or downloading material from internet sites that are likely to contain obscene, racist, hateful or other objectionable materials.
- 1.5 Downloading password recovery, cracking, security analysis or any other security software unless explicitly authorised by the Head of Information Security.
- 1.6 Intentionally interfering with the normal operation of the systems, including the propagation of computer viruses.
- 1.7 Causing sustained high volume network traffic that substantially hinders others in their use of the network (examples include web streaming).
- 1.8 The OU is under a statutory duty to have regard to the need to prevent people being drawn into terrorism. Should the use of OU computer equipment, information and Systems, give rise to a concern that a person may be at risk, this will result in action being taken in accordance with the OU Prevent Strategy.

4. Monitoring and blocking

- 4.1 The OU may use software tools to block sites that are obscene, hateful or have other objectionable materials, or may affect the University's operations.
- 4.2 For security and maintenance purposes, authorised individuals within the OU central IT teams may monitor any information, systems and network traffic at any time to ensure compliance with this and other security policies, and the effective operation of the University's systems.

Password Policy

Purpose

This document defines the password policy relating to OU information and information systems.

Scope

All users of OU information and information systems. For securing mobile devices, please refer to the Mobile Device Policy.

Policy

- 1.1 All passwords must be communicated separately from a user's OU Computer Username (OUCU).
- 1.2 First time passwords must be randomly generated and changed on first use.
- 1.3 Where systems capable, passwords must be a minimum of 8 characters and match 3 of the following conditions: uppercase, lowercase, numeric, and non-alphanumeric characters. Dictionary words should not be used to form a password.
- 1.4 Passwords must be set to expire automatically after a maximum of 90 days, prompting the user to create a new password.
- 1.5 Machine to machine accounts, otherwise known as service accounts, are exempt from expiry and consequently must be a minimum password length of 15 characters and match three of the following conditions: uppercase, lowercase, numeric, and non-alphanumeric characters.
- 1.6 User accounts must be set to automatically lockout for a minimum of 30 minutes after 8 failed logon attempts. IT Helpdesk is permitted to re-enable accounts upon request.
- 1.7 Users should be restricted from reusing the previous 12 passwords.
- 1.8 Passwords should be prevented from being changed more than once in a 24 hour period.
- 1.9 Computers and mobile devices must not be left unattended whilst unlocked and must be set to automatically lock after 15 minutes or less.
- 1.10 Passwords must not be shared, written down, recorded or printed.
- 1.11 The same password must not be used for multiple accounts across OU systems.
- 1.12 A password must be changed immediately if it has been discovered that the password has been compromised. If this is not possible, IT Helpdesk must be notified.
- 1.13 Passwords for information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).
- 1.14 Password reset must be implemented using a secure password reset mechanism.
- 1.15 Passwords must be stored using strong cryptographic techniques.
- 1.16 Failed logon error messages must not display the username or password.
- 1.17 Passwords must never traverse any network in plaintext, or utilising weak encryption.

Policies that apply to your work

Information Classification Policy

Purpose

The purpose of this document is to define the classification of OU information so that appropriate controls can be applied.

Scope

All users of OU information and information systems.

Policy

- 1.1 The Information Asset Owner of any information set created is responsible for assigning the appropriate information classification in accordance with this policy.
- 1.2 Information asset ownership may be transferred upon agreement with the newly identified Information Asset Owner.
- 1.3 OU information in any form must be managed in accordance with Information Security policies and the [Information and Records Management Policy](#).
- 1.4 Information Asset Owners should have an understanding of the administrative and technical controls for which they are accountable and responsible, and an awareness of those operated by IT, to safeguard information in accordance with its classification.
- 1.5 Where information has not received an information security classification, the 'Highly Confidential' classification must be assumed and applied.

Classification

Classification	Description	OU Specific Example
Highly Restricted	Information that requires controls above those implemented by the University to manage Highly Confidential information. Typically these controls are required for information types rarely handled by the University. For example, information where its loss could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations. Information of this nature would require specific controls that must be supplied by the Information Asset Owner, and must be adhered to by users of the information.	No normal line of business information falls into this category. Examples would include sensitive defence or medical research information.
Highly Confidential	Information that, if made public or inappropriately shared around the organisation, could seriously impede the organisation's operations and is considered critical to its on-going operations or the University's legal obligations under data protection regulations. Information may include accounting information, sensitive business plans, sensitive customer information of banks, solicitors and accountants etc., medical records and similar highly sensitive information. Such information should not be copied or sent to third parties without	Student personal details Staff Personnel records Some types of research information Sensitive business papers Banking details, payment card details (PCI)

	specific authority. Security at this level should be at the highest level for the University's normal operational requirements.	Organisational Risk registers containing confidential information Financial records Other items covered under data Protection Legislation. Alumni and Donor information
Proprietary	Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organisation operates. Such information is normally for authorised personnel only, for proprietary use. Security at this level is high.	Unit plans Operational plans Software and configuration specifications (unless given by agreement to open source communities) Analysis of anonymised student information.
Internal Use Only	Information not approved for general circulation outside the organisation where its loss would inconvenience the organisation or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include internal memos, minutes of meetings and internal project reports. Security at this level is controlled but normal.	Most committee minutes Unit hierarchies Depersonalised student information. Copyright protected Educational Resources
Public Documents	Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level is minimal.	Marketing information Open Educational Resources Open access research information and publications. University statistic and course information intended for public consumption

Acknowledged Information Asset Owners

Information asset ownership in the University is recorded by the University Secretary's Office and is described in the [Information roles and responsibilities](#) document guidance from the Academic Governance and Policy unit.

Access Control Policy

Purpose

This document defines the Access Control Policy relating to OU information and information systems.

Scope

All users of OU information and information systems.

Policy

Users' information and information systems

- 1.1 All users are required to sign a declaration that they agree to comply with the Computer Acceptable Use Policy, prior to using their computer account.
- 1.2 You may only use computers and computer accounts that you have been officially authorised to use.
- 1.3 Access to OU information and information systems must be granted through the provision of a unique username.
- 1.4 Users must not intentionally disclose their username to anyone outside of the OU.
- 1.5 Provisioned usernames grant access to OU information and information systems, and are required for a user's job role and responsibilities. Users must only access information for which they have appropriate authorisation.
- 1.6 The OU will actively monitor IT information systems for the detection and prevention of unauthorised access.
- 1.7 It is the responsibility of every user to report any unauthorised access to IT Service Delivery.
- 1.8 Information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Information Security Standard (PCI DSS).

IT administrators of information systems

- 1.9 Access Granted to university systems must follow the 'least privilege' principle, only granting access required for the user's job role.
- 1.10 Access to systems must be granted through a defined process, following an industry standard.
- 1.11 IT Service and Support Delivery will periodically review access permissions.
- 1.12 Administrator or 'root' access to OU information systems will be limited to staff whose job roles require it.
- 1.13 Administrator or 'root' accounts must only be used to facilitate tasks where elevated privileges are required.
- 1.14 For compliance, auditing and reporting purposes the use of generic IDs that are shared and not assigned to a specific named individual are restricted and should only be provisioned after an exception request is raised and approved.
- 1.15 Auditing of all active directory user accounts and permissions should take place at least once a year, in addition to checks on the use of privileged accounts.
- 1.16 Where possible, systems that cannot authenticate directly with active directory should use ADFS to accomplish a single sign-on for all systems.

Third party use of OU information and information systems

- 1.17 Public facing systems which facilitate access to Highly Confidential information will be subject to an Information Security risk assessment to assess if two-factor authentication is required.
- 1.18 For systems that do not use active directory to control access, it is the responsibility of the Information System Owner to conduct a yearly review of accounts and permissions granted.

Data Encryption Policy

Purpose

This document defines the Data Encryption Policy relating to OU information and information systems.

Scope

All users of OU information and information systems.

Policy

- 1.1 The OU will provide appropriate encryption capabilities for use on OU equipment.
- 1.2 Where passwords are used to secure encrypted data, users must adhere to the Password Policy.
- 1.3 Where a password or encryption key needs to be shared to enable another party to access encrypted information, the password or key must be communicated separately and securely.
- 1.4 Any data written to portable devices and storage from OU IT equipment must be encrypted.
- 1.5 All server management communications must be encrypted.
- 1.6 Information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).
- 1.7 The table below defines the minimum security controls required relative to the classification of information and should be adhered to at all times.

Technical Controls

<i>Controls</i>	Highly Restricted (exceptional level of sensitivity)	Highly Confidential (very high level of sensitivity)	Proprietary (high level of sensitivity)	Internal Use (moderate level of sensitivity)	Public (low level of sensitivity)
<i>Data Transmission</i>	On OU Network: Mandated by the Information Asset Owner	On OU Network: Encryption not required	On OU Network: Encryption not required	On OU Network: Encryption not required	On OU Network: Encryption not required
	Public Network: Mandated by the Information Asset Owner	Public Network: Encryption required	Public Network: Encryption required	Public Network: Encryption not required	Public Network: Encryption not required
<i>Data Storage</i>	On OU network: Mandated by the Information Asset Owner	On OU network: Encryption not required	On OU network: Encryption not required	On OU network: Encryption not required	On OU network: Encryption not required
	Third party storage: Mandated by the Information Asset Owner	Third party storage: Encryption required	Third party storage: Encryption required	Third party storage: Encryption not required	Third party storage: Encryption not required
	Portable devices and storage: Mandated by the Information Asset Owner	Portable devices and storage: Permitted with encryption for approved devices (See Mobile Device Standard for further information) only with restrictions	Portable devices and storage: Permitted with encryption for approved devices (See Mobile Device Standard for further information)	Portable devices and storage*: Permitted without encryption	Portable devices and storage*: Permitted without encryption

*Note that section 1.4 implements a stronger safeguard for some data types than stated in the table above to reduce the risk of incorrectly storing sensitive information

Media Disposal Policy

Purpose

This document defines the media disposal requirements relating to data stored on OU information systems media, including but not limited to electronic media (e.g. hard drives, USB memory sticks, memory cards, magnetic tape), optical media (e.g. Blu-Ray/DVD/CD) and hard copy.

Scope

All users of OU information and information systems.

Policy

- 1.1 Any optical media or hard copy classified as Proprietary or above must be destroyed using a shredder. Please refer to the Information Classification Policy for further details.
- 1.2 Where IT electronic media has been identified for disposal, the IT Service Delivery team must be contacted.
- 1.3 IT electronic media identified for disposal must be tracked in accordance with the Asset Management Lifecycle.
- 1.4 Where IT electronic media has been identified for reuse within the OU then the re-imaging of data storage devices must be undertaken.
- 1.5 Where computer and portable media has been identified for reuse outside the OU or for disposal, then a secure wipe to UK Government Communications Electronics Security Group (CESG) approved standards, must be completed by a CESG-approved third party.

Information Security Exceptions Policy

Purpose

The purpose of this policy is to define how exceptions to the Information Security policies will be managed.

Scope

All users of OU information and information systems with the exception of the use of publicly accessible, externally presented systems.

Policy

- 1.5 Exception to Information Security policies will be considered where there is a justified requirement and the additional risk and/ or cost to mitigate that risk can be balanced with the business benefit.
- 1.6 For an exception to be considered an [Information Security Policy Exception Request Form](#) must be completed.
- 1.7 All exception requests will be considered and processed by IT Information Security.
- 1.8 Approved exceptions to policy requests will be logged and regularly reviewed.

Information Security Incidents Policy

Purpose

This document defines the Incident Response Policy to minimise the impact to the OU information and information systems.

Scope

All users of OU information and information systems.

Policy

- 1.1 All users of OU information systems are required to report any identified information security incidents, or observed or suspected security weaknesses in systems or services to the IT Helpdesk.
- 1.2 Network and system components must be configured to alert system administrators of security incidents as defined in the Network Configuration Standard.
- 1.3 An Information Security Incident Response Plan must be maintained and aligned to unit incident plans and tested by the Information Security Team and circulated to all relevant parties.
- 1.4 The OU will maintain the capability to detect and respond to the unauthorised access, disclosure, modification or loss of information on OU information systems.
- 1.5 The Information Security Incident Response Plan and incidents relating to information systems which process, store and/or transmit payment card information must adhere to all applicable requirements in the Payment Card Industry Data Security Standard (PCI DSS).

Policies that apply to you when working outside the office

Mobile Device Policy

Purpose

The purpose of this policy is to define the secure use of mobile devices within the OU to protect the University's information and information systems.

Scope

This policy applies to devices including but not limited to smart phones, tablets, laptops and removable storage referred to herein as 'mobile devices', either personally owned (Bring Your Own Device – BYOD), or supplied by the OU, which connect to the OU networks or are used to access or store OU information classified as Internal Use Only or above.

Policy

- 1.1 Mobile devices must be secured using a passphrase, PIN number or a pattern lock which is not easily guessable.
- 1.2 Mobile devices must be set to wipe all data after a maximum of ten unsuccessful login attempts.
- 1.3 Mobile devices must not be left unattended whilst unlocked and must be set to automatically lock after 15 minutes or less.
- 1.4 Mobile devices must have an up-to-date operating system and anti-virus protection.
- 1.5 Mobile devices must not be 'Jailbroken' or 'rooted', or have otherwise circumvented the installed operating system security requirements.
- 1.6 Information which is stored on the mobile device (including any removable storage) and is classed as Proprietary or above, must be protected via encryption.
- 1.7 Mobile Device Management (MDM) technology will be used by the OU to enforce this policy and block access if required. Only mobile devices used in conjunction with MDM technology and configurations as described in the IT Mobile Device Standard may be used to send or store classified information.
- 1.8 If a mobile device has been lost or stolen, it must be promptly reported to the IT Helpdesk and where necessary, IT Service Delivery will take steps to protect OU data from unauthorised access by remotely wiping the device.
- 1.9 The OU cannot see any of your personal data on mobile devices, however the OU reserves the right to monitor and log data traffic transferred between mobile devices and OU systems.
- 1.10 Personally owned mobile devices must not access the OU Staff wireless network, but can access the eduroam or TheCloud wireless networks.
- 1.11 Personally owned mobile devices must not retain personal information from OU information systems.
- 1.12 Personally owned mobile devices must be returned to the manufacturer's default settings before they are sold, exchanged or disposed of. All OU information must be securely wiped as part of this process.
- 1.13 Mobile devices are not permitted to connect to the Payment Card Industry Data Security Standard (PCI DSS) segregated network.

- 1.14 The OU will use posture checking to ensure that OU-issued devices and personal devices which request to connect to the internal network meet policy requirements.
- 1.15 The OU reserves the right to deny or restrict access to any mobile device that does not meet policy requirements. This is to preserve the confidentiality, integrity and availability of the OU network and its systems.

Remote Access Policy

Purpose

This document defines the policy for remotely accessing devices connected to OU information systems from external networks.

Scope

All users of OU information and information systems.

Policy

- 1.1 Any computing device connected to an Open University network, either directly or via a remote access technology must not be accessible to remote users unless authorised by the Open University IT department.
- 1.2 Remote access to OU devices will only be granted through solutions provisioned and supported by the OU IT department.
- 1.3 Remote access to Open University networks from any equipment is permitted provided it satisfies security criteria of the remote access solutions.
- 1.4 Remote access to Open University networks must be from IT equipment using a vendor-supported operating system, and up-to-date security patches and antivirus software.
- 1.5 All requests for remote access must be raised with IT Helpdesk for approval.
- 1.6 OU user accounts with administrator or 'root' level privileges must not be used for remote access unless specifically required for support purposes.
- 1.7 Tokens and/or PINs that facilitate two-factor authentication must not be stored with related IT equipment.
- 1.8 Remote access will be restricted to only those IT information systems or resources that users have been granted permission. No attempt should be made to circumvent any restrictions.
- 1.9 The OU will actively monitor all remote access sessions for the detection and prevention of unauthorised access.
- 1.10 Resources that are in scope of the Payment Card Data Security Standard (PCI-DSS) require stringent security controls. Consequently remote access to PCI-DSS in scope resources is not permitted.
- 1.11 Non-console, remote administrative access onto card data environment (CDE) hosts, should use multi-factor authentication.

Policies that apply to you if you work with third party suppliers

Third Party Services Security Engagement Policy

Purpose

This document defines the policy for engaging with and managing third party service providers who connect, process, store and/or transmit OU information.

Scope

Third parties and all users of OU information and information systems.

Policy

1. Engagement

- 1.1 All third parties working on behalf of the OU must be assigned a sponsor.
- 1.2 Consultation with the Information Security Team and/or the Unit Information Security Liaison Officer should be carried out as early as possible in order to ensure that appropriate due diligence is undertaken, and to identify if a risk assessment is required to ensure that the University is not exposed to undue risk.
- 1.3 When engaging with a third party for the first time, a Non-Disclosure Agreement (NDA) must be signed before any OU information is disclosed.

All third parties engaged to provide services to the OU must have a contract in place. Third party engagement must comply with the University's [Procurement Policy and process](#)

- 1.4 The contract must include the following:
 - Confidentiality clause
 - Agreement to follow all OU Information Security policies
 - Right to audit clause
 - Secure disposal of OU information upon termination of contract.
- 1.5 All third parties who process personal data on behalf of the University must have a data processor clause written into the commercial contract. The Data Protection Office should be contacted for further information. All external transfers of personal data from the University to the supplier and from the supplier to other approved parties must be recorded by the supplier and the Data Protection Office.
- 1.6 The sponsor is responsible for ensuring that; the appropriate agreements and contracts are in place; the third party access rights to information and information systems are provisioned in accordance with the Information Asset Owner's approval and that where software development is outsourced to a third party, requirements of the Secure Software Development Policy are implemented.
- 1.7 All contracts with third parties for the supply of services to the University will be monitored and reviewed to ensure that information security requirements are being satisfied.

- 1.8 Third parties must notify the OU of any security incidents impacting OU information or information systems within the terms specified in the Service Level agreement (SLA)

2. Third party access connections or interfaces to OU systems

- 2.1. All third party connection requests must have approval from the following; Sponsor, Information Asset Owner, IT Service Delivery, and Information Security before being granted.
- 2.1. Where third party access is granted, connectivity must be provisioned through approved OU solutions, restricted to the resources required to carry out the work.
- 2.2. Third party connections must be terminated when no longer required and may be terminated in the event of a security breach.
- 2.3. The OU will monitor third party connections for the detection and prevention of unauthorised access.
- 2.4. A central register of all third party connections will be maintained by IT Service and Support and will be reviewed and updated quarterly or as necessary.
- 2.5. Third party access to information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).

Policies that apply to you if you take card payments

Payment Card Policy

Purpose

This document defines the Payment Card Policy relating to OU information and information systems.

Scope

All users of OU information and information systems.

Policy

- 1.1 The storage of cardholder data as defined by the Payment Card Industry Data Security Standard (PCI DSS) is strictly prohibited.
- 1.2 Information systems which process and/or transmit payment card information must adhere to all applicable requirements mandated in the PCI DSS.
- 1.3 It is the responsibility of all project managers and sponsors to ensure that projects are compliant with the PCI DSS Standard where applicable.
- 1.4 Wherever possible, systems should restrict interfacing directly with the cardholder data environment (CDE) to limit the necessary scope of PCI DSS compliance.
- 1.5 Card payments may only be accepted using methods approved by the OU Finance Division.
- 1.6 Each person who has access to payment card data is responsible for protecting the information.
- 1.7 Any suspected or actual information security breach resulting in the compromise of payment card data must be reported immediately to IT Helpdesk.
- 1.8 The payment card Primary Account Number (PAN), which is typically 16 digits in length, must never be sent and/or received via email or instant messaging and should be automatically detected and blocked wherever possible.
- 1.9 A list of all authorised devices and personnel with access to the PCI DSS in scope resources must be maintained by IT and Treasury Services Finance.
- 1.10 Non-console, remote administrative access into the card data environment (CDE), should use multi-factor authentication.