University of Liverpool

Workspace and IT Equipment Security Policy

Reference Number	CSD-004
Title	Workspace and IT Equipment Security Policy
Version Number	1.0
Document Status	Active
Document Classification	Open
Effective Date	03 December 2014
Review Date	28 March 2018
Author	Computing Services Department (David Hill)
Approved by	Corporate Services & Facilities Committee
Implemented by	Information Security Officer
Monitoring of compliance	Faculty Information Security Managers (Local) CSD Information Security (Central)
Comments	• **03/12/2015 - Annual Review** • **03/12/2016 – Annual Review** • **28/03/2017 – Annual Review**

Table of Contents

1. Introduction

Information is a vital asset to any organisation, and this is especially so in the University which is a knowledge-driven organisation. Virtually all of our activities create information assets in one form or another, or are used, transmitted and stored via IT equipment.

2. Principles

The policy ensures that individuals who have a legitimate right to use, store and access University IT and electronic assets can do so, whilst ensuring that information is protected at all times from unauthorised or malicious access.

This policy helps all staff and students of the University to ensure that assets are used, transmitted and stored correctly using appropriate methods:

- All information assets must be handled and managed in accordance with their classification;
- Assets should be made available to all who have a legitimate need to access them;
- The integrity of information must be maintained; information must also be accurate, complete, timely and consistent with other related information and events;
- All staff and students who have access to information assets are responsible for handling them in accordance with their classification;
- Information asset owners are responsible for ensuring that the University classification scheme is used appropriately.

3. Objectives

The objectives of this policy are to:

- Define the responsibilities of individuals for safeguarding University IT and information assets;
- Provide a rigorous and consistent protection system which ensures University assets are appropriately protected and managed in accordance with both relevant legal requirements and University policy;
- Ensure any IT and information assets which are lost, stolen, damaged or intercepted are sufficiently protected and unreadable to mitigate the risk of loss of data;
- Minimise any potential damage to the University, its customers and partners as a result of IT information assets being intercepted or exposed.

4. Implementation

Procedures will be put in place to ensure that this policy is effective. These procedures include:

- Appropriate identification of University staff and students to enable access to information/equipment for which they have a legitimate need;
- Identification and protection of information assets and IT equipment , facilitated by the correct categorisation and use of handling methods for those assets;
- Developing adequate control mechanisms to protect information assets, e.g. use of University IT services;
- Implementing and reviewing access control mechanisms for authorised staff, students and visitors; and

- Safely and securely disposing of all information assets and equipment.

5. Data Protection Act 1998 (DPA)

The DPA requires the University to ensure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

For more information please refer to the University's Information Security Policy and Data Protection Policy for more information.

6. University campuses and surroundings (physical access)

Authorised staff, students and visitors

Access to University premises and facilities is limited to those who have been authorised to have access and have been provided with a valid ID card. University staff and students must:

- Carry their ID card whenever entering University premises;
- Safeguard their ID card at all times and report its loss or damage immediately; and
- Supply, on request, any necessary details for a temporary ID card to be issued for use on those occasions where an individual's own ID card has been forgotten;

Any staff/student who fails to provide relevant identification/evidence may be refused physical entry to University premises.

Access passes must differentiate between staff/students and visitors within University premises.

Visitors must be met either at a designated reception area or by a University staff member at a building's main entrance and a visitor's attendance and departure must be recorded.

Any University staff or student, whom suspects and/or witnesses unauthorised entry to University premises must report it immediately to the University Security Services.

Telephone: 0151 794 2222 (external) or 2222 (internal) – telephone service available 24/7

Sensitive buildings and areas

Buildings and work spaces, that are considered sensitive or critical to University business, require an appropriate level of access control in order to protect them against unauthorised access, interference and damage. Access controls include swipe card access, CCTV, physical locks and barriers.

University buildings may require additional physical security controls or a physical security reviews. For initial advice and more information please contact Facilities Management Security Services.

Access to sensitive areas (Data Centre/communication rooms/machine rooms)

Authorised staff, students and visitors may have access to specific sensitive areas which are critical to IT services and day to day activities. Staff, students and visitors must be authorised prior to accessing sensitive areas such as data centres, communication rooms, machine rooms, PC centres and cluster areas.

Access to sensitive areas managed by Computing Services is restricted to individuals who have been granted authorisation as part of their day to day role. Should access be required please contact the CSD Service desk in the first instance.

7. Acceptable usage

To ensure the security of devices, equipment and data, each authorised staff, student or visitor that uses, stores, and creates University information and IT assets must be aware of and accept:

- University IT Regulations
- Janet(UK) Acceptable Use Policy
- Information Security Management System (ISMS)

8. Sensitive research and use of IT

In carrying out research and study, IT usage may occasionally require viewing, searching, downloading material and participating with specific groups that would otherwise raise suspicion of wrong doing and trigger a security incident and/or investigation from appropriate authorities.

Sensitive research and data may relate to:

- Terrorism/extremism/religious and ethical beliefs
- Military and government related works (Official Secrets Act)
- Material which is sexual or violent in nature
- Vulnerable or disempowered individuals
- Medical/test participation (human/animal)

Any staff or student who requires the use of University IT equipment (PC/laptop/Internet use or other) for sensitive research purposes must complete and submit a Sensitive IT Usage Form and/or complete a Research Ethics application.

The use of University IT equipment in these circumstances will also be communicated to appropriate authorities, as necessary, with details of the nature and intended purpose of the research.

Failure to supply this information may precipitate an investigation into an individual by an external authority which, in extreme cases, may result in criminal proceedings.

9. Physical security (including workspaces)

University Information and IT equipment which is used, created, processed, stored, transmitted and accessed on University premises and remotely (working from home and/or in public places) **must be secure at all times,** including when:

- Left unattended;
- In the presence of unauthorised staff/student(s), visitors and third parties; and
- In transit, including when leaving University premises.

Information delivered verbally (including by telephone and through voicemail)

Any private or sensitive information which is communicated verbally must be conveyed in a secure area to prevent eavesdropping. Sensitive information which is delivered verbally must be conveyed within a private area or meeting room away from public spaces.

Voicemail must be protected by a PIN which has been changed from the default PIN. Please refer to guidance from CSD to learn more about managing your voicemail effectively and securely.

Internal and external mail

Written items sent through internal or external postal systems must be securely packaged and correctly addressed. Where appropriate, confirmation of receipt should be requested. Courier services which require a signature to be recorded on receipt (e.g. Special/Recorded delivery) should be used where possible.

Controls for receiving, storing, and distributing mail must be in place where mail is to be delivered to an individual address or to a location without a secure, central, sorting point. These controls may include:

- Locked communal mailboxes (key/code) accessed by authorised staff /students;
- Secure drop-off by Third party delivery (Recorded/non-recorded) services, e.g. Royal Mail, TNT, DHL etc., should the recipient be unavailable;
- Ensuring the accuracy of postcodes and address details for University buildings.

For more information on secure mail please refer to Facilities Management Mail Services.

IMPORTANT – Facilities Management are not responsible for the day to day physical attendance and security of the mail. It is the responsibility of individual departments and schools.

Clear desks and screens (including workspaces, whiteboards, and printers)

Sensitive data and IT equipment must be protected at all times **before, during and after** use/creation/processing. Sensitive data and IT equipment must never be left unattended at any time.

Staff and students must ensure that:

- Their workspace is clear of any paper or files containing sensitive information
- Sensitive information and IT devices/equipment are locked away, to prevent unauthorised access, e.g. Payment Card Processing equipment (PDQ's), PCs and Laptops
- Sensitive information which has been produced on whiteboards or noticeboards of any type is not available to public view
- All workspaces (offices, cabinets and drawers) are locked when not in use or prior to leaving the workspace
- Sensitive documents and files are collected immediately during and upon completion of processing

Particular care and attention must be paid by those working in open plan offices, meeting rooms, publicly accessible buildings and other areas with high levels of traffic.

Please refer to the Information Asset Classification Policy for details about how workspaces and working areas may be classified.

10. Removal of University Assets

University assets must never be removed from University premises without agreement from the designated authoriser.

It is the responsibility of authorisers to adequately protect University assets at all times and to ensure that they are returned in the same condition in which they were supplied.

If you are travelling abroad on University business, including undertaking work or research outside the UK/EU, check the Information security advice and guidance for the country you are visiting prior to travel.

11. IT equipment, network and storage security

Asset Tags/Registration

All IT equipment which has been purchased through University channels must have asset tags attached and be registered within the Computing Services Asset Inventory. The Inventory records each asset's usage and details of the individual responsible for it. Where practical, University asset tags must be visible on IT equipment to clearly illustrate that it is University property.

Asset tags must not be removed from any University IT equipment. If an asset tag is not visible or has been damaged, it is the responsibility of the individual who is responsible for that equipment to arrange with CSD for a new asset tag to be attached.

IT equipment

This policy applies to all system and technology whereby data is stored and processed. This includes but is not limited to:

- PCs
- Laptops
- Mobile phones/tablets
- Landline phones
- External and removable media resources e.g. CDs/DVDs/USB/External Hard Disk Drives (HDD)

When using IT equipment you must adhere to the following guidance:

- Ensure sensitive activities are undertaken within secure areas provided by the University
- Physically secure IT equipment within specific sensitive areas (e.g. using locks/swipe access/CCTV) where unauthorised staff/students and third parties have access to shared University rooms/offices/buildings
- Never allow unauthorised University staff/students to view, access, tamper or manipulate University information assets and IT devices
- Always visually check for miscellaneous or foreign hardware that may be connected to IT equipment before logging on
- Never leave IT equipment and removable media within a unsecured area where malicious activity could take place or where there is the potential for loss, damage or interference by intruders (e.g. coffee shops/unsecured car parks/public roads and streets)

- Any configuration of University-owned IT equipment must be undertaken by the Computing Services Department
- Unauthorised staff/students must not install any software on University IT equipment
- Staff/students must avoid writing down passwords
- Ensure ALL default passwords/PINs are changed prior to use, e.g. voicemail
- Only share encryption keys with authorised staff/students where encryption has been undertaken and/or is required - encryption keys must not be shared/sent via University email (including webmail)
- IT equipment connected to the University network must conform to the appropriate specifications (including current security updates) and run only those protocols supported by the University
- University IT equipment, including external storage devices, must be password protected and encrypted where sensitive data and usage is undertaken away from secure areas (such as remote working away from the University)
- Always lock your computer screen and ensure that you use appropriate settings to secure your system/screen when away from your workspace
- Ensure the recommended security software and patches are installed on IT equipment at all times
- Staff/students must never disable services or security controls on devices which have been pre-configured by Computing Services (including antivirus, firewall and encryption)

Email

- Computing Services will never ask for your password: staff/students must never share passwords or respond to any request asking for such details
- Send sensitive data encrypted through University email (includes Webmail)
- Never respond to, forward, or send unsolicited items (including chain, spam or socially engineered emails)
- Staff and students must not, under any circumstances, monitor, intercept or browse other users' email messages (unless authorised to do so as part of day to day activities)
- If there is a considerable amount of sensitive data to be sent to a third party then files should be sent through Secure File Transfer Protocol (SFTP) or other secure means
- Defamatory views, statements and opinions about other staff/students must be avoided at all times
- Copyrighted material must not be distributed without prior permission from the copyright owner(s)
- University accounts, including email addresses, should not be used to sign-up to third party web applications and services for personal use (including, but not limited to, content sharing sites such as YouTube, and social media channels such as Facebook)
- Ensure an out-of-office message is in place during pre-arranged leave to ensure urgent queries can be redirected and that any University business can be attended to accordingly

Storage/Backup

- Always store University-owned data via University provided secure storage (such as M drive / departmental drives)

- In the event there is a requirement for a separate backup service staff/students must refer to the CSD provided PC/Mac Tivoli service/DatAnywhere services in the first instance
- Sensitive data must have secure and controlled at all times, e.g. through access permissions (restricted, or read-only) and encrypted/password-protected

Network/Web Services

- All IT equipment connected to the University network must conform to the appropriate specifications (including current security updates/software) and run only those protocols supported by the University - equipment which does not comply will be prevented from accessing the network until corrective action has been taken
- Access to the University network must be authorised through the use of a secure user name, password AND further authentication (where required) for accessing sensitive services, data and communications, e.g. via VPN/SSL/HTTPS
- When working off-site, or undertaking sensitive research, always connect to University services designed to securely support these activities, such as the Virtual Private Network (VPN) and Apps Anywhere
- The only authorised protocol to be used across the University network is TCP/IP
- Only one workstation may be connected to each network socket. In particular, the use of a network hub, switch, router or wireless access device (or any similar device) to connect multiple workstations to a single network connection is not permitted (unless there is sufficient justification AND authorisation from Computing Services)
- Unauthorised equipment will be blocked from accessing the University network. This includes all ancillary network equipment not owned or registered with Computing Services
- Never connect, intercept or monitor the University network, its services and/or its staff and students
- Never remove/change or introduce a service to the core infrastructure network (MWS) without prior approval from Computing Services
- All network addresses, including IP addresses, will be allocated and administered by Computing Services
- Any non-Computing Services/University e.g. third party, which requires a connection to the core network or changes to the configuration of the network - including firewall - must be requested via a Service Provider Security Review Form, reviewed and authorised by the relevant faculty and professional security officer

12. Passwords, online security and encryption

For information and guidance on choosing, changing and protecting your passwords and for guidance about staying safe online please refer to the links below for more information:

Password security	http://www.liv.ac.uk/csd/security/passwords/
Online security	http://www.liv.ac.uk/csd/security/online-security/
Encryption	http://www.liv.ac.uk/csd/security/informationsecurity/encryption/
Email security	http://www.liv.ac.uk/csd/security/email-security/
Mobile security	http://www.liv.ac.uk/csd/security/mobile-security/

13. Secure disposal

IT equipment including PCs, laptops, telephones, mobile phones, and printers must be disposed of in a secure manner with a certificate of destruction maintained for audit purposes. For more information please refer to the IT Asset Disposal Policy.

For paper documents, staff and students must use secure methods provided by the University. These include:

- Cross cut shredders;
- Confidential waste bins; and
- Approved Document Disposal Services

14. Social media

Please refer to the Social Media Compliance Policy for more information.

15. Security incident response

In the event of suspected loss or damage to University assets please refer to the Information Security Incident Response Policy.

16. Security investigation

Please refer to the Security Investigations Policy for more information.

17. CSD Service desk contact details and service times

The Computing Services Service desk can be contacted in the first instance for all problems and queries relating to IT services and software. The Service desk can be contacted using several methods including:

- Logging an online support request: http://servicedesk.liverpool.ac.uk/
- Email: servicedesk@liverpool.ac.uk
- Telephone: 44567 (internal)
- Telephone: +44 (0) 151 794 4567 (external)

18. Legal obligations and University policy

This policy is aimed at all members of the University who have a responsibility for the use, management and ownership of information assets. This policy is part of the University Information Security Management System (ISMS) and should be read in conjunction with the Policy and its sub-policies and relevant UK legislation. Further relevant policies and legislation are listed in Appendix A.

19. Compliance and Monitoring

Members of staff are bound to abide by the University IT regulations by the terms of their employment. Students are bound to abide by the University IT Regulations when registering as a student at the University.

Authorised staff members of the University may monitor the use and management of information assets to ensure effective use and to detect unauthorised use of information assets.

Appendix A (University ISMS)

- Regulations for the Use of IT Facilities at the University of Liverpool
- JANET Acceptable Use policy
- Information Security Policy
- Workspace and IT Equipment Security Policy
- Information Security Incident Response Policy
- Information Asset Classification Policy
- Information Security Review Policy
- IT Procurement and Third Party Security Policy
- Procurement Policy
- Data Protection Policy
- Freedom of Information Policy
- Copyright Policy
- Card Payment Policy
- Records Management Policy
- Records Retention Policy
- Risk Management Policy
- Student/HR Disciplinary Procedures

Relevant legislation includes:

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Data Retention Investigatory Powers Act 2014
- Counter Terrorism and Security Act 2015 (Prevent)
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002

Relevant Regulation includes:

- PCI-DSS (Payment Card Industry Data Security Standards)