Loughborough University

Information Security

# Policy Pack

## Contents

Policy 1 ... Information Governance Policy *2*
Policy 2 ... Introduction to Information Security *6*
Policy 3 ... Information Categories and Controls Policy *11*
Policy 4 ... Responsibilities of All Staff and Research Students *14*
Policy 5 ... Information Service and Service Contractors Policy *18*
Policy 6 ... Mobile Working Policy *22*
Policy 7 ... Information Sharing Policy *27*
Policy 8 ... Policy on the Management of User Access to Information *34*
Policy 9 ... IT Operations Management Policy *40*
Policy 10 . Management of Information Security Incidents and Review of Policies *52*

Loughborough
University

Information Security

# Information Governance Policy

Approved
June 2016

www.lboro.ac.uk

# Information Governance Policy

## 1. Summary

Information is a vital asset to the University. It underpins the University's Research, Teaching and Enterprise. It is fundamental to all other activities associated with its staff, students, funders, collaborators, and strategic partners as well as the efficient management of all its services and resources. It plays a key part in governance, planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

## 2. Principles

The University recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The University fully supports the principles of good corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal and commercially sensitive information that is held by the institution. The University also recognises the need to share information and data with other organisations and other agencies in a controlled manner consistent with the interests of our staff, students, funders, collaborators and strategic partners and, in some circumstances and where appropriate, with the public.

The University believes that accurate, timely and relevant information is essential to deliver the highest quality in all its activities.

There are 3 key interlinked strands to the University's information governance policy:

- Openness
- Legal compliance
- Information security

### 2.1. Openness

- Non-confidential information on the University and all its activities should be available to the public through a variety of media. This may include through: open access publishing, the institutional repository, Freedom of Information Act compliance, etc.
- The University adopts a general policy of openness in terms of allowing individuals access to their personal information. Personal information will be maintained and released to the individuals concerned on request in accordance with the provisions of the Data Protection Act.
- The University has clear procedures and arrangements for liaison with the press, on-line and broadcasting media through its Marketing and Advancement function.

- The University will have clear procedures and arrangements for handling queries from our staff, students, funders, collaborators, strategic partners, suppliers and the public.
- The University will support the effective sharing of data where appropriate.

### 2.2. Legal Compliance

- The University regards all identifiable personal and commercial information relating to its staff, students, funders, collaborators, and strategic partners and as processed in the course of its research activities as confidential, except where relevant legislation requires otherwise.
- The University will undertake or commission regular and appropriate assessments and audits of its compliance with legal requirements.
- The University has established and will maintain policies to ensure compliance with all relevant legislation.
- The University has established and will maintain policies for the controlled and appropriate sharing of information with other agencies, taking account of relevant legislation.

### 2.3. Information Security

- The University will establish and maintain policies for the effective and secure management of its information assets and resources.
- The University will undertake or commission regular and appropriate assessments and audits of its information and IT security arrangements.
- The University will promote effective confidentiality and security practice to all its staff, students, partners and suppliers through policies, procedures and/or training as appropriate.
- The University, through the Information Governance Sub-Committee of the Information Technology and Governance Committee will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and information security.

## 3. Responsibilities

It is the role of the University Council to approve the University's policy in respect of Information Governance, taking into account legal and Higher Education Sector requirements. Council is also ultimately responsible via the Chief Operating Officer for ensuring that sufficient resources are provided to support the requirements of the policy.

The Information Technology and Governance Committee, comprising representation from across the University, with support from the Information Governance Sub-Committee, is responsible for overseeing Information Governance policy and planning, developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the University and raising awareness of Information Governance.

Staff and students are expected to take ownership of, and seek to improve, the quality of information within their specified areas of activity. There is also an expectation that this policy and its supporting standards and guidelines are built into local processes and procedures and that there is on-going compliance.

All staff, whether permanent, temporary or contracted, and contractors/suppliers are responsible for ensuring that they are aware of the requirements incumbent upon them in and for ensuring that they comply with these on a day to day basis.

Specific responsibilities of key staff will be found in Annex 1.

This policy document will be reviewed on an annual basis by the Information Governance Sub-Committee of the Information Technology and Governance Committee.

# Annex 1 Staff Responsibilities

## 1. Chief Operating Officer

The Chief Operating Officer (COO) is responsible to the Vice-Chancellor on a delegated basis for the general oversight and development of information governance policy. The COO has responsibility for ensuring policies and procedures are implemented and that mechanisms are established to monitor their effectiveness.

## 2. Deans of Schools and Heads of Professional Services

Deans of Schools and Heads of Professional Services have responsibility for the implementation of University information governance policies and procedures in their Schools and Services. The Dean or Head of Service should demonstrate visible commitment to good information governance by:

a) Ensuring that all staff undertake the general training in good information governance practice provided by the University.

b) Ensuring that staff undertake specialised information governance training relevant to their roles (e.g. research data management).

c) Ensuring that there are systems in the School or Service to maintain awareness of the information held and to ensure it is stored, used and shared only in accordance with University policies and procedures.

d) Providing sufficient resources for staff to be able to comply with University policies and procedures.

e) Bringing to the attention of the COO, any breach of statutory requirements which cannot be dealt with at School/Service level and/or may have implications for the University more widely.

f) Ensuring that staff co-operate fully with any information or information security audits authorised by the Information Technology and Governance Committee.

g) Ensuring students and staff are aware of the School or Service’s procedures for secure handling of their personal data.

h) Ensuring that University information governance policies and procedures are followed in any dealings, formal or informal, with third party individuals and organisations.

Loughborough
University

Information Security

# Introduction to Information Security

Approved
June 2016

# Introduction to Information Security

## Introduction

The University's Information Governance Policy notes the key role which information plays across the full range of the work of the University. Staff, students and some external partners need to access information and the University's information systems to carry out their daily activities. The University also provides a range of information for the public. The University recognizes the need for an appropriate balance between openness and confidentiality in the management and use of information. To achieve this aim and ensure the University complies with its legal responsibilities, a suite of information security policies has been developed to guide staff, students and external partners on how to use and handle University information whilst maintaining a level of confidentiality appropriate to the nature of the information. The policies are also relevant to members of the public who may wish to access information about the University.

## Purpose and Key Definitions

This policy provides an introduction to the University's Information Security Policy Framework and includes links to all policies in the Framework.

By **Information** we mean any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphical, cartographical, narrative, or audiovisual.

By **Information Security** we mean the management of information to allow appropriate access and use for those who need it whilst preventing unauthorized access which might result in a breach of the University's legal responsibilities, the rights of individuals or might present a reputational risk to the institution. It includes arrangements to reduce the risk of copying, modification or deletion of information where this is not legitimate for the conduct of University activities.

The term "**the University**" in the Policy Framework should be interpreted in the widest sense and includes relevant activities, services and systems related to all Schools and Professional Services of the University as well as related to IT Services.

The risks to maintain good information security may be deliberate or accidental human acts, or arise from technical or environmental factors.

**Confidentiality** - Confidentiality is the need to ensure that information is disclosed only to those who are authorised to view it.

**Information Systems** – Any system, service or infrastructure used to process information or the physical locations housing them. This includes critical business environments, business processes, business applications (including those under development), computer systems and networks.

**Personal Data** – Any data held in a system, whether electronic or hard copy, that identifies a living individual (for a legal definition, see the Data Protection Policy

www.lboro.ac.uk/admin/ar/policy/dpact/ludpp ).

**UCISA** – Universities and Colleges Information Systems Association

www.ucisa.ac.uk/

## Scope

This policy provides a framework for the management of information security throughout the University and applies to:

- All those with access to University information and information systems, including staff, students, partners and contractors;
- Any systems attached to the University IT or telephone networks and any systems supplied by the University;
- All information  stored or processed by the University for its operational activities, regardless of whether it is stored or processed electronically or in hard copy form, including any communications sent to or from the University and any University information  held on systems external to the University network;
- All external and third parties that provide services to the University in respect of information processing facilities and business activities.

## Aims

The Information Governance Policy sets out the following principles for Information Security:

- The University will establish and maintain policies for the effective and secure management of its information.
- The University will undertake or commission regular and appropriate assessments and audits of its information and IT security arrangements.
- The University will promote effective confidentiality and security practice to all its staff, students, partners and suppliers through policies, procedures and training as appropriate.
- The University, through the Information Governance Sub-Committee of the Information Technology and Governance Committee will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and information security.

The University is committed to protecting the security of its information and information systems in order to ensure that:

- The integrity of information is maintained, so that it is accurate, up to date and ‘fit for purpose’;
- Information is always available to those who have a legitimate need for it and there is no disruption to the business of the University;
- Confidentiality is not breached, so that information is accessed only by those authorised to do so;

- The University meets its legal requirements, including those applicable to personal data under the Data Protection Act;
- The reputation of the University is safeguarded.

The policy framework structure is based on the “UCISA Information Security Toolkit” which, in turn, is based around the ISO 27000 series standards. It provides guidance on the Information Categories and Controls for different types of information (Public, Not Sensitive, Confidential, and Confidential) and a series of policies aimed at both general (e.g. All Staff and Research Students) and more technical audiences (e.g. IT Operations Policy).

The University is committed to providing training to ensure staff, students and partners understand the importance of information security and, in particular, exercise appropriate care when handling Confidential and Highly Confidential information. It also provides specialist advice when required.

# Responsibilities

The Information Governance Policy sets out the responsibilities of key University bodies and senior staff in relation to Information Security. The responsibilities of all staff and research students and of taught students are set out in the relevant policies below.

Training and specialist advice on information security is available from Academic Registry and IT Services (M.Lister@lboro.ac.uk).

## IT Governance Committee and Information Governance Sub-Committee

The Information Technology and Governance Committee (ITGC)

http://www.lboro.ac.uk/committees/it/

with support from the Information Governance Sub-Committee (IGSC), is responsible for:

- Ensuring that users are aware of this policy;
- Seeking adequate resources for its implementation;
- Monitoring compliance;
- Conducting regular reviews of the policy, having regard to any relevant changes in legislation, organisational policies and contractual obligations;
- Ensuring there is clear direction and visible management support for security initiatives.

# Information Security Policy Framework

The Information Security Policy Framework sits under the overall Information Governance Policy and is made up of the following sub-policies:

- Introduction to Information Security (this policy) (relevant to all)
- Information Categories and Controls Policy (relevant to all)
- Responsibilities of All Staff and Research Students
- Responsibilities of Taught Students (Acceptable Use Policy)
- Information Services and Service Contractors Policy (relevant largely to IT professionals or others involved in procuring IT related services)

- Information Sharing Policy (relevant to all)
- Mobile Working Policy (relevant to all)
- Policy on the Management of User Access to Information (relevant to all)
- IT Operations Policy (relevant to IT professionals)
- Information Security Incident Handling and Review Policy (relevant to all)

The following policies are also relevant to all staff and students (taught and research):

- Data Protection Policy
- Freedom of Information Policy
- Copyright Policy
- Software Policy

Loughborough University

Information Security

# Information Categories and Controls Policy

Approved
June 2016

# Information Categories and Controls Policy

## 1. Purpose

The right level of security can only be applied to information if those creating, storing, processing and potentially sharing the information are conscious of how sensitive and confidential the information is. To aid structured thinking about this issue and for use within other information security policies, a categorisation scheme for University information is set out below.

## 2. Scope

This policy is relevant to all staff, students and third parties that have access to University information and the relevant University information systems.

Given the volume of information held in the University, users are not expected to physically label all information with one of the Categories below. However, they are expected to be familiar with the Categories and to use them to inform their working practices. All Highly Confidential category information should be labelled as such given the need for extreme security measures for its handling.

## 3. Information Categories and Handling

The table sets out the information categories used at Loughborough University and the required approach to handling information in each category. The format in which the information is held may be electronic or hardcopy.

| Category | Examples | Control Measures |
|---|---|---|
| **1. Public**<br>**Available to anyone anywhere in the world regardless of their connection with the University** | Already published information (e.g. public University website):<br>Prospectuses, newsletters etc.<br>Charter, Statutes, Ordinances & Regs<br>Most general policies & procedures<br>Staff Research interests<br>Open Access Research Data<br>Job vacancies<br>Contact details for public staff roles | Can be disclosed or drawn to the attention of anyone.<br>For most purposes, the format should preserve the integrity of the information (e.g. share in PDF format rather than Word/Excel). However, open access research data will be made available in a readily analysable form (e.g Excel, .csv, Word or .txt)<br>Contact details will be for specific public-facing roles only. |

| Category | Examples | Control Measures |
|---|---|---|
| **2. Not Sensitive**<br>**Information which is not pro-actively published but which is not confidential or sensitive**<br>**Can be shared openly amongst staff, students and third parties on request.** | Some internal procedural/operational Documentation<br>Some Committee papers/review documents/discussion papers which are not openly published (especially after the elapse of time)<br>Statistical reports where there are no competitive issues<br>Internal non-confidential research reports | May be stored in any formats and systems which are efficient for the user/process concerned.<br>If shared, the format should preserve the integrity of the information where appropriate (e.g. Marketing information/official institutional information should be shared in PDF format rather than Word/Excel).<br>It would be good practice to seek the consent of the originator before circulating further. |
| **3. Confidential**<br>**Unauthorised disclosure would cause a breach of legal responsibilities, financial and/or reputational damage to LU or to the individuals involved.**<br>**May be shared internally and externally on a restricted and secure basis.**<br>**This category includes most information defined as confidential in Section 27 of the Academic and Academic Related staff Conditions of Service - unless such information falls within the Highly Confidential category below.** | Personal staff and student data, including medical information, disciplinary information, PDRs, information on ethnicity or religion etc. This is referred to as ‘Sensitive Personal Data’ by the Data Protection Act (1998)<br>Research data or other intellectual property covered by confidentiality agreements or with potential for commercial exploitation by LU (Theses, dissertations etc.).<br>Commercial contracts or information relating to their negotiation.<br>Sensitive policy/committee documents/correspondence (e.g. relating to major changes/new developments/discontinuation of activities, financial issues)<br>Examination papers prior to examinations being taken. | Should be stored in secure, password protected and normally corporate IT systems (or locked locations if hardcopy)<br>May be shared between authorised staff and students for legitimate business purposes.<br>May be shared with third parties where appropriate permission has been given (personal data) or where covered by explicit agreements between relevant parties (e.g. research collaborations, funding bodies etc.)<br>See further info on secure storage and information sharing in Staff Responsibilities and Information Sharing policies. |
| **4. Highly Confidential**<br>**Exceptionally confidential information which would cause major financial loss, and reputational damage or significant distress to the data subject if used in an unauthorised manner.**<br>**A very limited number of individuals will have access.** | Information obtained or generated through a partnership covered by the Official Secrets Act or a contract/partnership requiring extreme security measures (e.g. some NHS data). | A specific agreement will set out the individuals with access and will detail data storage, sharing mechanisms and working practices. |

Information Security

# Responsibilities of All Staff and Research Students

Approved
June 2016

# Responsibilities of All Staff and Research Students

## 1. Purpose

This policy outlines the responsibilities of all staff and research students in relation to information security and provides links and direction to other, relevant Information Security Policies.

## 2. Scope

This policy is relevant to all staff and research students. The responsibilities of taught students have been incorporated into the Loughborough University IT Acceptable Use Policy.

The University's Introduction to Information Security Policy provides a brief overview of the approach and some useful definitions.

This policy should be read in conjunction with the Loughborough University IT Acceptable Use Policy

www.lboro.ac.uk/services/it/staff/help/policies/aup/

and in accordance with the University Data Protection,

www.lboro.ac.uk/admin/ar/policy/dpact/ludpp/

Freedom of Information

www.lboro.ac.uk/admin/ar/policy/foi/

and Copyright Policies.

copyright.lboro.ac.uk/copyright/policy/copyright-policy/

Individuals with third party access to University information should refer to the Project Partners guidance (in preparation) but may also find this policy helpful.

## 3. Roles and Responsibilities

It is the responsibility of all staff and research students to read and comply with the Acceptable Use Policy and all other Information Security Policies as approved by the University. Senior staff members have additional responsibilities which are listed in the Information Governance Policy.

The University will provide relevant training to all staff and research students. It is the responsibility of all individuals to complete the mandatory Information Security training and attend any bespoke sessions offered which are relevant to their specific roles and activities.

Staff and Research Students should store, handle and process information in accordance with the Information Categories and Controls Policy. In the event that individuals are unsure as to what category the information they are handling should be considered, then further clarification should be sought from the Data Owner (as set out in the Information Sharing Policy) to ensure that the appropriate level of security is applied to it. If information is considered to be either Confidential or Highly Confidential, then it should be handled in accordance with the Information Categories and Controls Policy. In particular personal data about individuals must be handled in accordance with the University's Data Protection Policy.

www.lboro.ac.uk/admin/ar/policy/dpact/ludpp/

Staff and Research Students should ensure that information is stored appropriately and in accordance with the Information Categories and Controls Policy. Electronic Confidential information should be stored in a secure environment (e.g. workspace, encrypted laptop). Hardcopy Confidential information should be stored in a lockable facility. Access to Confidential information must only be granted in accordance with the Policy on the Management of User Access to Information. When entering into data storage agreements with third parties and external organisations, it is the responsibility of all individuals to do so in accordance with the Information Service and Service Contractors Policy.

Staff and Research Students should ensure that information is shared only in accordance with the Information Sharing Policy and when consent has been provided by the data owner (examples of data owners can be found in the Information Sharing Policy). In this context, individuals should be aware of the University's Freedom of Information Policy and seek advice from their line manager or the Freedom of Information Officer if information is requested (the release of which might represent a reputational or commercial risk to the University).

Staff and Research Students should ensure they are aware of the University's Copyright Policy and that their actions do not constitute a breach of copyright ownership. Advice is available from the Copyright Specialists in the Library.

copyright.lboro.ac.uk/copyright/policy/copyright-policy/

When handling information away from your main location of work (whether on or off campus) - and/or when working via a personally owned device, staff and research students must act in accordance with the Mobile Working Policy. Particular care should be taken when handling Confidential information in these circumstances.

Staff and Research Students should ensure that their actions do not represent a risk to the effective operation, security and integrity of the University IT systems and environment. The University's Software Policy is particularly relevant in this context

www.lboro.ac.uk/services/it/staff/help/policies/software/

and University IT Professionals must be consulted should access to non-University maintained software be required.

Staff and Research Students should notify the University if they become aware of a data breach or are concerned that information is not being handled in accordance with the Information Security Policies. In the first instance, concerns should be raised with the appropriate line manager or supervisor. However, in some cases, it may be necessary to notify Information Security staff of the concern. Please refer to the Management of Information Security Incidents and Review of Policies document for further guidance on this.

Failure to comply with the Information Security policies may be treated as misconduct and could be subject to disciplinary action as per University Ordinance XVII (students)

www.lboro.ac.uk/governance/ordinances/17/current/

and Ordinance XXXV (staff).

www.lboro.ac.uk/governance/ordinances/35/current/

Loughborough University

Information Security

# Information Service and Service Contractors Policy

Approved
June 2016

# Information Service and Service Contractors Policy

## 1. Policy Overview

To provide some elements of its IT infrastructure and corporate and local IT systems cost effectively, the University works with a range of external partners. For example, IT solutions may be hosted by systems operated by the partner, information systems such as Agresso and iTrent are supported under contract with the company which develop and maintains them. Also remote monitoring services may be purchased from a partner organisation. As part of the contracts relating to these services, third party organisations are likely to require physical and/or remote access to University information and systems.

To ensure the security and integrity of University information and systems, this policy sets out the conditions for providing access to third party organisations in the contractual context outlined above. It should be read in conjunction with the Management of User Access to Information policy which covers authorization of individual access to information and systems.

## 2. Policy Audience

The majority of this policy applies to IT Services and Facilities Management staff. Schools and other Professional Services within the University should also use this policy when procuring services which require providing access to locally managed information or physical and/or remote access to locally managed infrastructure, information or systems.

This policy applies to:

- Service Providers – These are external to the University, and may maintain systems on the University's behalf. Service Providers are likely to require remote access to University information systems.
- Service Contractors – These are external to the University, and may host systems externally on behalf of the University. Service Contractors are likely to require access to University information to provide a service.

This policy should be referenced:

- When third party organisations are involved in the design, development or operation of information systems for the University. There may be many reasons for this to happen, including installing and configuring commercially developed software, third party maintenance or operation of systems, to full outsourcing of an IT facility. (Service Provider)
- When access to the University's information systems is granted from remote locations where computer and network facilities may not be under the control of the University. (Service Provider)

- When users who are not members of the University are given access to information or information systems. (Service Provider)
- When a service is outsourced to a third party which involves University data being hosted at an external location outside the control of the University. (Service Contractor)

## 3. Policy Sections

The policy section has been separated depending on the type of service.

## 4. Service Provider

Staff responsible for agreeing service, maintenance and support contracts will ensure that the contracts being signed are in accordance with the University's Information Governance Policies. This will require review of the relevant policies and procedural documentation of the partner organisation.

Service owners/managers must assess the risk to the information and services to be covered by the contract. If Confidential information is to be shared the service provider will be required to sign a confidentiality agreement. Access to Highly Confidential information will not be given to service providers unless the arrangement is part of the initial contractual arrangements relating to the information. Should any changes be required subsequently, the authorization of all relevant parties must be obtained and documented in advance of any changes to previously agreed arrangements for ensuring the security of the Highly Confidential information.

If a service is being procured which requires that a third party has enhanced access to critical University infrastructure, the contractual terms must be approved and signed by the Chief Operating Officer before implementation of the service.

Physical access to locations which are deemed high value security risk areas (e.g. locations containing core networking equipment) must be arranged in advance and service providers must be accompanied in these locations at all times by a member of University Security, Facilities Management or IT Services personnel.

Where remote access to information systems is required, the Remote Access to Server(s) Procedure needs to be followed by the service provider conducting the work. The following information will be required:

- Remote IP address which will be used to connect to the University's information systems;
- Primary contact in the organisation, including name, job title, telephone number and email address.

Forms can be found at:

https://internal.lboro.ac.uk/it/dept/Teams/Network-and-Security/Remote%20Access%20Procedure/

Completed forms should be forwarded to the IT Service Desk.

Prior to the service provider conducting any work, a detailed change request must be completed. Only if the request is approved under the IT Services Change Management Process will access be granted.

Standard user accounts (-remote accounts), which have no administrative privileges, will be provided to service provider staff to allow access under the Management of User Access to Information policy. Only protocols approved by IT Services will be authorised for use and usage will be monitored and logs retained as per the data retention period.

Staff responsible for agreeing and approving changes must ensure that all changes made are logged for auditing requirements.

## 5. Service Contractor

Staff responsible for agreeing service, maintenance and support contracts will ensure that the contracts being signed are in accordance with the University's Information Governance Policies. This will require review of the relevant policies and procedural documentation of the partner organisation.

Service owners/managers must assess the risk to the information and services to be covered by the contract. If Confidential information is to be shared the service provider will be required to sign a confidentiality agreement. Access to Highly Confidential information will not be given to service providers unless the arrangement is part of the initial contractual arrangements relating to the information. Should any changes be required subsequently, the authorization of all relevant parties must be obtained and documented in advance of any changes to previously agreed arrangements for ensuring the security of the Highly Confidential information.

When transferring data to the Service Contractor, unless the information falls into the Public or Not Sensitive information category, the transfer should be conducted via a secure means (encrypting the data first).

Prior to procuring external hosted services, where relevant detailed information should be obtained from the external contractor and reviewed by IT Services. This is to ensure that the contractor is capable of handling the University's information securely. Examples of the type of information required can be found in Appendix A.

# Appendix A: Example questions for External Contractors

- Is the service contractor ISO27001 certified?
  This certification formally specifies a management system that is intended to bring information security under explicit management control.
- Can the service contractor provide a copy of their information security policy?
  This policy would outline the management controls that are in place to manage information security.
- Can the service contractor provide a copy of their data retention policy?
  This would indicate the length of time the contractor would hold the University's information.
- Is the service contractor on the Data Protection register?
  Every organization that processes personal information must notify the Information Commissioner's Office. This information is then held in the form of the Data Protection Register.
- If the service contractor is going to be processing electronic payments on behalf of the University, are they PCI DSS compliant?
  PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This standard is intended to help organisations proactively protect user account data.
- Is the service contractor subject to regular security testing (penetration testing) or Information Security audit?
  This is to ensure that service contractors, which are certified against any information security standards, are still compliant. Penetration testing will ensure that the contractors' infrastructure is secure.
- Can the service contractor ensure that all web applications, which leverage the University information will be conducted via secure web (HTTPS)?
  This is to ensure that if Confidential information is involved in the service provision it is communicated securely.
- Does the contract include appropriate Data Protection assurances in-line with EU Data Protection equivalency requirements? As controls change frequently, please contact the IT Service Desk for advice.

Loughborough University

Information Security

# Mobile Working Policy

Approved
June 2016

# Mobile Working Policy

## 1. Policy Overview

This policy sets out the expected working practices and safeguards to be followed by individuals when working “on the move” and away from their desk or work station on one of the University campuses. It covers the use of both University owned devices and personally owned devices for mobile working and recognizes that such working may take place on the University campus, but away from the individual’s main base, or elsewhere in the UK or internationally including at the individual’s home address.

## 2. Policy Audience

This policy applies to all members of staff and students. It also represents the practice expected of third party individuals working in partnership with the University who have access to University owned information and who are accessing that information away from a secure environment on one of the University’s campuses.

## 3. Home Working

Staff may be permitted to work at home in line with the University’s Home Working Policy and specific arrangements should be agreed with their line manager.

Both University and personally owned devices may be used for home working and information security risks will need to be considered carefully in the context of the University’s information security policies depending on the nature of the information to be accessed, the device(s) to be used and the nature of the home environment. In the rest of this policy the term mobile working is taken to include home working.

## 4. Use of Personally Owned Devices

The University recognizes the benefits brought by use of personally owned devices and equipment. They facilitate legitimate working from home and help individuals to manage varied workloads wherever they are located on or off campus. Examples of such devices include:

- Desktop computers (typically at home)
- Laptops
- Tablet computers
- Smart Phones
- Smart Watches

## 5. Use of Personally Owned Devices in countries that prohibit use of encrypted devices

You should not take encrypted devices into countries that prohibit use of such equipment unless you are happy to unencrypt the device.

## 6. Responsibilities of all Staff and Students when using Personally Owned Devices – Set Up of Device

If you use your own device to access University information or to conduct activities related to your role within the University you must:

- Ensure that you adhere, at all times, to the Acceptable Use Policy;
- Familiarise yourself thoroughly with the device and its security features so you are able to ensure the safety of University information (as well as your own);
- Ensure that separate accounts are used on devices shared with family members;
- Ensure that all relevant security and anti-virus features are enabled, where appropriate;
- Maintain the device yourself ensuring both the Operating System and additional software (Apps) are regularly patched and upgraded;
- Set appropriate passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device and will be enforced by appropriate IT Systems;
- Devices must be encrypted where possible (note that Apple mobile devices are encrypted automatically if at least the 4 digit PIN is enabled);
- Take responsibility for any software that is downloaded onto the device;
- Set up location tracking services and remote wipe facilities where available until central IT services are available which will enforce the option to erase at least the email content;
- Ensure that Confidential Information is not retained on the device for longer than is necessary;
- Ensure that Highly Confidential information not stored on the device;
- If Confidential or Highly Confidential information is at risk report any loss or theft of the device to IT Services and implement a remote wipe, if possible;
- Ensure that when a personally owned device is disposed of, sold or transferred to a third party all University information is securely and completely deleted from it by following the procedures which IT Services Helpdesk should provide;
- For disposal of all University owned devices, please ensure that all WEEE guidelines at the following link are followed (note: separate procedures for laptops and for mobile phones): http://www.lboro.ac.uk/services/sustainability/waste/weee/

Details of how to access University IT facilities such as email through your own device will be found on IT Services webpages http://www.lboro.ac.uk/services/it/email/

The University takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee-owned devices, or for any loss or damage resulting from any support and advice provided.

## 7. Working Practices

This section is applicable to use of information from University and personally owned devices and some clauses are also relevant to hardcopy information.

When working away from campus, and when available, the use of the international eduroam wireless service should be used for security reasons and to avoid additional expensive wireless and mobile roaming costs. Further details are available at: http://www.lboro.ac.uk/services/it/out/eduroam/

The majority of wireless networks, including those in coffee shops and hotels, are shared and therefore malicious people can view some of the activity happening on your device. It is therefore essential to use the University Off Campus VPN or Remote Working Portal when working on Confidential or Highly Confidential University information, and it is recommended as standard practice. Further details are available at:
http://www.lboro.ac.uk/services/it/out/off-campus/

You should not use devices owned by third parties to access or process University information (e.g. Internet Cafes) unless these third parties are trusted partners whose relationship with the University is covered by a formal agreement e.g. research partners).

As you would when you are working on campus at your normal work location, when working on a mobile basis you should always ensure that unauthorized individuals cannot see or access Confidential or Highly Confidential University information (as defined in the Information Categories and Controls Policy).

You must take all reasonable steps to:

- Prevent the theft or loss of information;
- Ensure that no unauthorised access to Confidential or Highly Confidential information can take place, paying due regard to the provisions of the Data Protection Act and the University's Data Protection Policies as well as any commercial agreements which may relate to the information you are accessing or processing;
- Maintain the integrity of information, ensuring that relevant information is copied back to central University information systems where appropriate;
- Ensure that no University information is left on any personal device indefinitely (see above).
- Report any security breach immediately to IT Service desk in accordance with the Information Security Incident Handling Policy.

## 8. Monitoring and Access

The University will not monitor the data content of your personal devices unless the data is stored or synchronised with University systems (email, workspaces etc), however the University has the right to monitor and log data traffic transferred between your device and University systems, both over internal networks and entering the University via the Internet.

The University also reserves the right to:

- Prevent access from a particular device from either wired or wireless networks or both;
- Prevent access to a particular system;
- Disable user accounts if deemed to have been compromised;
- Take all necessary and appropriate steps to retrieve information owned by the University.

From time to time, the University may require that you install or update University-approved device management software on your own device.

## 9. Information Sharing

Please see the Information Sharing policy for guidance on the use of Removable Electronic Media, Cloud Services and third party facilities for collaborative working and information sharing with external partners.

## 10. Loss, Theft or Damage of Device

If a device is damaged, lost or stolen that holds Confidential or Highly Confidential information belonging to the University, this should be reported to the IT Service desk, regardless of whether the device is University or personally owned. Staff should make all possible enquiries to attempt to locate lost or stolen devices and report any potentially criminal activity to the appropriate authorities.

In the event that a personally owned device is used to access or share University owned information, then the University reserves the right to remotely wipe the device in the event that it becomes damaged, lost or the University becomes concerned that the security of the information has been compromised.

Loughborough
University

Information Security

# Information Sharing Policy

Approved
June 2016

# Information Sharing Policy

## 1. Policy Overview

The work of the University requires the sharing of information between staff, between staff and students, and between staff and (external) third parties. This policy section aims to minimise the risk of loss, unauthorised disclosure, modification or removal of information maintained by the University whilst seeking to maintain the open nature of the organisation. The majority of this policy covers information categorised as Confidential under the University's Information Categories and Controls Policy.

## 2. Policy Audience

This policy applies to all members of staff, students and third parties who have access to Loughborough University information.

## 3. Scope

This policy covers the sharing of information, which has been categorised at different levels under the University's Information Categories and Controls Policy, and the mechanisms used to share such data. It covers all forms of information, whether held and shared in hardcopy or electronic format.

Routine sharing of information happens regularly as part of day to day activities at the University. Examples include circulating and/or providing access to documents via workspaces (i.e. job application packs, meeting packs) or sending general emails. In these cases, information may ultimately be accessed both via University owned and non-University owned/maintained electronic devices (please see below).

The guidance in this document covers those day to day activities as well as examples of more obvious sharing of information. For example:

- Research data is shared with colleagues both internal and external to the University (third parties) as part of a collaboration or agreement
- Information is shared with the police in response to a legitimate request (i.e. under the Data Protection Act).

Information sharing may also happen as part of automated IT processes and the process owner is responsible for ensuring the sharing complies with the guidance within this policy document.

# 4. General Guidance

As indicated in the Information Categories and Controls Policy, staff should be mindful of the category of information they are handling. In outline, the degree of control required over sharing is as follows (based on the information category):

1. Public Information – May be disclosed or drawn to the attention of anyone. For most purposes, the format should preserve the integrity of the information and should not reveal previous changes (e.g. share in PDF format rather than Word/Excel). However, open access research data will be made available in a readily analysable form (e.g. Excel, .csv, Word or .txt) following the removal of “Hidden Data” (contact IT Services Helpdesk for advice).
2. Not Sensitive – May be generally shared but it would be good practice to seek the consent of the originator before doing so. The format in which the information is shared should normally retain the integrity of the information without revealing previous changes made to it (e.g. PDF or hardcopy format rather than Word/Excel – which may reveal tracked changes and/or previously saved copies of drafts).
3. Confidential – May be shared internally, and with authorised third parties/research students, for legitimate reasons but, given the categorisation, careful consideration is required before deciding to do so. Likewise, the format in which the information is to be shared should also be given careful consideration.
4. Highly Confidential – A specific agreement will detail those individuals who should have access to the information and will detail data storage, sharing mechanisms and working practices that should also be in place.

Draft documents should normally be considered as ‘Confidential’ until they have been finalised or approved through the relevant line management or governance arrangements.

Where a decision is taken to share information, it is the responsibility of those releasing the information to ensure that the recipient understands the confidentiality of the information and will abide by the provisions of this policy.

The remainder of this policy relates to the sharing of Confidential information.

# 5. Data Owner

All information within the University should have a Data Owner. The Owner is responsible for risk management and it is therefore the responsibility of the Data Owner to assign this information to a category (as per the Information Categories and Controls Policy), and provide advice and guidance on how the information should be accessed or shared, in accordance with the overarching Policy Framework. Being the Data Owner is not the same as being the owner of the Intellectual Property. Additionally, the Intellectual Property in the information may be held by someone who is not the Data owner. All staff should be aware of their individual responsibilities for handling data in the four categories above.

Examples of data owners:

- A document created by a member of staff on an aspect of their job for their own use. The data owner of this document is the member of staff who created it;
- Principle Investigators (PI) on research projects are the Data Owners of research data created or collected during the project.

- The data held within LUSI (student records system). The data owner for this data is the Academic Registrar;
- The data held within Agresso (finance system). The data owner for this data is the Director of Finance;
- Research data provided to the University by an external body. In the case of research projects, data may be shared or transferred with or from external bodies, and the rules governing the ownership, sharing or transferring will be determined by the Research Collaboration Agreement.

In some cases, it is possible that the data owner may delegate data owner responsibilities to other members of staff, but ultimately they remain the data owner.

Individuals or groups analysing, or otherwise, making use of (including publishing) information categorised as 'Not Sensitive', 'Confidential' or 'Highly Confidential' must ensure they have the permission of the Data Owner in advance. This permission may be clear through standard working practices or through the agreements in place related to specific projects. However, it must be sought on a case by case basis when any unusual or non-standard use is to be made of University information. If ownership is not clear, this should be referred to the Information Governance Sub-Committee for guidance.

## 6. Sharing in Hardcopy Format

Sharing of Confidential Information in hardcopy form is discouraged as further sharing by the recipient remains easy and there is considerable risk of this information not being maintained or disposed of securely. If such sharing is undertaken, checks should be made on the arrangements for appropriate storage and disposal, and these should comply with the Policy on the Management of User Access Information and Retention Policy]

## 7. Sharing in Electronic Format

Information is most frequently shared in electronic format. Such formats make information easy for recipients to share, potentially when it is not appropriate to do so. Wider sharing than that which is absolutely necessary and informal arrangements for version control also increase the risk that information will be stored in multiple locations, potentially in different versions and that it will be retained for longer than is appropriate. To enhance information management and reduce risk of loss of Confidential information staff are advised to consider carefully the electronic media they employ for sharing with authorised recipients.

For sharing Confidential information with other individuals with University accounts, the use of the IT workspace service with appropriately controlled access is strongly recommended. Sharing through this mechanism restricts access and removes the risks associated with creation of multiple copies.

Confidential information can be shared through storage in corporate information systems where those systems are known to have restrictions on access (e.g. the storage and sharing of confidential information about students in Co-Tutor or LUSI and on staff through iTrent).

Where sharing is necessary with individuals who do not have access to the above systems such as external partners, and it would not be appropriate to give them such access, individuals may use a Cloud Service but must follow the advice provided below.

## Email

As with other forms of electronic format, care should be taken when sharing information via email. This policy acknowledges that sharing Confidential information between University staff and students is essential for the conduct of day to day activities.

If possible Confidential information should not be shared via email attachment to email addresses outside of the University, as once shared, copies of documents will no longer be held within a corporate information system (e.g. a document is no longer situated within a secure workspace, or University's email system) and can no longer be deemed secure.

Where it is essential for the conduct of University business to share external confidential information via email, it is recommended that a password is used to encrypt the Microsoft Office or Adobe PDF document and a suitable disclaimer included in the email:

*"This message (including any attachments) may contain confidential, proprietary, privileged and/or private information. The information is intended to be for the use of the individual or entity designated above. If you are not the intended recipient of this message, please notify the sender immediately, and delete the message and any attachments. Any disclosure, reproduction, distribution or other use of this message or any attachments by an individual or entity other than the intended recipient is prohibited."*

All users are advised to follow the steps identified in the 'Email Good Practice' document.

## Cloud Services

The use of cloud-based storage makes collaboration and sharing of information very easy and convenient. Increasingly, cloud-based storage is more cost effective than services being provided on site by the University.

Where possible, confidential information should only be stored or shared onsite or via cloud-based storage services managed by IT Services, this is currently Microsoft One Drive and Arkivum (providing research data storage).

However, it is recognised that projects and services which involve external partners may require the sharing of Confidential information using other Cloud based information storage systems.

The following best practice advice should be applied when using cloud-based storage systems that are NOT managed by IT Services, for example:

- Dropbox;
- SpiderOak;
- Google Drive;
- Amazon Cloud Drive.

If there is any doubt about the categorisation of the information, advice should be sought from information governance staff in the Academic Registry. IT Services may be asked to advise on appropriate sharing technology where information is Confidential or Highly Confidential. Where cloud-based storage is the only viable option, users of such services **MUST** ensure:

- The software licensing terms or an explicit contract is held between the University and the service provider that includes appropriate Data Protection assurances in-line with EU Data Protection equivalency requirements. As controls change frequently, please contact the IT Service Desk for advice.
- Cloud-based storage is only to be used with the approval of the data owner;
- All confidential information is encrypted prior to being stored, transmitted or shared (please contact IT Services for current guidance on the procedure for encrypting documents);
- No encryption passwords are stored within the same storage provider;
- Decryption of encrypted information must never take place within the cloud environment;
- For research data, any relevant contractual terms are consulted and complied with, as some organisations prohibit the use of cloud-based storage for research data;
- When sharing Confidential information, passwords are not shared via unsecure channels such as email;
- The encrypted version of the information is not the sole source and that secure back-ups are stored on an IT Services managed location;
- Once the sharing of the Confidential information is no longer required, that it is removed from the cloud-based storage.

## Other Electronic Media

The use of other electronic media other than email and workspace services for sharing Confidential or Highly Confidential material is discouraged as they increase the risk of inappropriate sharing or loss of Confidential information. However, the use of such media is not prohibited.

## Mobile/Removable Storage and Devices

These are defined as all types of electronic storage which are not physically fixed inside a computer or laptop; or the device itself is easily moved. They include the following:

- Memory cards (like those used in cameras), USB pen drives etc.;
- Removable or external hard disk drives;
- Newer Solid State (SSD) drives
- Mobile devices (iPod, iPhone, iPad, MP3 player);
- Optical disks i.e. DVD and CD;
- Floppy disks;
- Backup Tapes.

If saving and sharing information via one of the above media is considered to be essential as it is deemed to offer significant advantages over use of one of the previously recommended, more secure approaches, the user must ensure:

- That anti-virus software is present and up to date on machines which data is taken from and machines which data is transferred to;
- Only information, which has been categorised as not being Confidential is transported unencrypted on standard devices.

Information on anti-virus software and encryption of information is available at www.lboro.ac.uk/services/it/staff/software/personal/staffantivirus/

and users should also refer to the Encryption policy, section 8. The University is moving to encrypting all laptops by default.

Users wishing to transport and/or share Confidential information using electronic media MUST also ensure:

- The data on the device is encrypted to the highest recommended encryption standard (AES-256). Please contact IT Services for further assistance, or visit : http://www.lboro.ac.uk/services/it/staff/specialist/security/kingston/
- Compliance with any certified level of encryption required under a research or other grant or contract (e.g. to a standard such as FIPS-140-2). If such requirements are stipulated, please contact IT Services for further assistance;
- Mobile devices and/or electronic storage devices containing Confidential information should not be sent off site without the prior agreement of the data owner. IT Services should be consulted to ensure the level of security is appropriate for the type of data being transferred;
- Electronic media used to store Confidential information shall only be used by authorised individuals and where there is a clear business need;
- Data stored on the electronic media is the responsibility of the individual who operates the device.
- That electronic media should not be used to store information which is not securely backed-up in a central location as should the encryption password be forgotten, the information will be irretrievable.
- That the electronic media is physically protected against loss, damage, abuse or misuse when in use, storage and transmit.
- That should any electronic media holding confidential information become damaged, it should be given to local IT Support or IT Services staff for secure disposal.
- That the University (IT Services) is notified in the event that the device is lost or stolen.
- That when the business purpose has been satisfied, the information is securely removed/deleted through a destruction method that makes the recovery of data impossible.

Where electronic media containing Confidential information needs to be posted to third parties; services that provide tracking and auditing must be used. The decrypting password should not be in the same package as the media in question. Passwords should normally be provided to third parties either in person or via a telephone call.

In the event that a personally owned device is used to access or share University owned information, then the University reserves the right to remotely wipe the device in the event that it becomes damaged, lost or the University becomes concerned that the security of the information has been compromised. (Also see policy on Mobile Working).

Loughborough
University

Information Security

# Policy on the Management of User Access to Information

Approved
June 2016

# Policy on the Management of User Access to Information

## 1. Policy Overview

Loughborough University implements physical and logical access controls across the: IT Systems, data networks, and information it holds in order to provide authorised, auditable and appropriate user access; and to ensure appropriate preservation of: data confidentiality, integrity and availability.

Access Management systems are in place to protect the interests of both those who have provided information to the University and authorised users of that information.

## 2. Policy Audience

This policy document applies to:

- Staff in management roles who are responsible for authorising access rights appropriate to individuals in their areas of responsibility;
- Authorised users (new starters, current users);
- Leavers;
- Authorised users moving jobs or changing responsibilities;
- Service providers requesting access to information held by the University, IT Systems or network access;
- Authorised external stakeholders (e.g. research partners).

The majority of this policy applies to user accounts, which are created and managed within IT Service;, but the same principles should be applied across the whole University when granting access to information, regardless of its format..

## 3. Policy Sections

### Authorisation of Access

Deans and Heads of Professional Services are responsible for ensuring that there are systems in their School or Service to maintain awareness of the information held and to ensure it is stored, used and shared only in accordance with University policies and procedures (2(c) of the University Information Governance Policy).

It follows that Schools and Professional Services must have mechanisms through senior staff and line managers for the authorisation of appropriate access to information by members of the School or Professional Service whether that information is held in the School or accessed through University systems and regardless of the format of the information. In relation to access to information held in corporate IT Systems, the School must have arrangements to ensure authorisation to individuals complies with the access approval procedures for the specific system concerned.

These expectations also apply to the management of access to information by service providers and external stakeholders.

Access rights should be authorized following the principles of least privilege and need to know.

## Access in Hardcopy Format

Confidential information held in hardcopy format should be kept in locked storage which cannot easily be removed from the room concerned (e.g. locked filing cabinets, safes). Only staff authorised to access the information should have access to the key and they should be provided with specific training to ensure they are aware of their responsibility for maintaining the confidentiality and integrity of the information concerned.

When Confidential information is being used, staff should take care that its content is not visible from ground floor windows and that unauthorised individuals within the building do not have access to it. Rooms should be locked when empty and unauthorised staff should not be left alone in the presence of Confidential information.

## User Accounts

All members of staff, as defined by the University's HR system (iTrent), have an IT account automatically created for them on their appointment and are issued with an initial password. This IT account will be linked to an assigned telephone number and telephone directory entry.

All students of the University, as defined by the Central Student Record System (LUSI), have an IT account automatically created for them when they complete the on-line student registration process and are issued with an initial password.

The majority of IT systems will utilise this central IT account; therefore, it is important to ensure you keep the password securely and use the account in accordance with the University IT Acceptable Use Policy.
http://www.lboro.ac.uk/services/it/staff/help/policies/aup/

The User Accounts of staff leaving the University will remain active for 30 days after their last working day. However access to some University systems will be removed from the date of contract termination. Further information can be found at
http://www.lboro.ac.uk/services/it/staff/new/registration/faqs/

Any additional authorised users at the University who require access to IT Services facilities and services will be provided with an IT account on request and with suitable authorisation (contact IT.Services Helpdesk for advice.)

## Account Types

The different types of accounts which can be requested via IT Services is available in Appendix 1 below.

## Generic accounts

Generic accounts (many individuals sharing a single username and password) shall not normally be permitted as a means to access Loughborough University data, but may be granted under exceptional circumstances if sufficient additional controls on access are in place. Under all circumstances, users of accounts must be identifiable at all times. The business case and control arrangements will be agreed between the relevant School or Professional Service manager and IT Services before the account is created.

Generic accounts will never be used to access information categorized as Confidential or Highly Confidential under the University's Information Categories and Controls Policy.

## Third Parties

Third parties (Service providers, contractors and project partners) will be provided with accounts if necessary that solely provide access to the systems and / or data relevant to their relationship with the University, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or partnership agreement and will be reviewed at least on an annual basis by the IT Service Desk.

## Privileged accounts

The allocation of privileged rights (e.g. local administrator, domain administrators, root access) to information systems shall be managed by IT Services in consultation with School and Service staff with relevant responsibilities. Deans of Schools and Heads of Professional Services must ensure appropriate arrangements are in place for allocation of privileged access rights to any local systems.

Privileged accounts must only be used by systems administrators when undertaking specific tasks which require special privileges. Systems administrators must use their user accounts at all other times.

## Keeping Information Secure

Every user should understand the sensitivity of the information to which they have access in accordance with the University's Information Categories and Controls Policy and treat it accordingly. Even if technical security mechanisms fail or are absent, every user should attempt to maintain the security of data based on its information category.

## Access to Highly Confidential and Confidential information

Access to Highly Confidential or Confidential information will be limited to authorised persons whose job or study responsibilities require it, as determined by law, contractual agreements or the Information Governance Policy.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources within Loughborough University's Active Directory infrastructure managed by IT Services.

## Management of User Privileges

Management of user privileges should wherever possible be based on group membership or role assignment rather than individual accounts although this will not be appropriate for access to some Highly Confidential information.

A user's access to information systems must be controlled and updated by relevant managers and system administrators when circumstances change. This is to ensure that security risks are minimised and to allow University business to continue without undue hindrance.

- Users' access rights must be adjusted in a timely manner to provide only that access which is authorised and necessary.
- The purpose and membership of all privileged groups and roles should be periodically reviewed by the business owner.
- A periodic general review by the business owner of login accounts should lead to removal of access to those accounts, which are no longer eligible or required.

## Compromised accounts and passwords

If a University user account or password is suspected to have been compromised, the incident should be reported immediately to the IT Service Desk, who will follow the appropriate process. Such passwords must be changed as soon as possible. Appropriate arrangements should be made for this eventuality with local systems in Schools and Professional Services.

## Misuse of Systems Access

The University can at any time suspend a user’s access to a corporate system if it is believed they are sharing account details, conducting malicious or illegal activities.

The Acceptable Use Policy
www.lboro.ac.uk/services/it/staff/help/policies/aup/

sets out the purposes for which University systems may be used (whether provided by IT Services or locally). Misuse of systems or abuse of access to other University information by staff or students may be treated as a disciplinary offence. Use of systems or University information in relation to criminal activity by staff, students or third parties will be reported to the police.

## Appendix 1 – Account Types available from IT Service

| Account type | Services available | Account characteristics |
|---|---|---|
| -admin | No services offered | This type of account is provided when a user needs to administer a particular service.<br>This account is created within the directory service provided by IT Services and permissions are granted on the authority of the appropriate service owner. |
| -extra | No services offered | This type of account is provided when a user has been authorized to administer their local computer/laptop.<br>This account is created within the directory service provided by IT Services and access is granted on the local computer/laptop. |
| -remote | No services offered | This type of account is provided to external service providers, to allow for remote management of systems or services.<br>This account is created within the directory service provided by IT Services and permissions are granted once a completed remote access document has been received and signed off by the service owner. |
| -svc | No services offered | This is a service account which is created when a particular service requires access to domain services.<br>This account is created within the directory service provided by IT Services and permissions are granted on the authority of the appropriate service owner. |
| Temporary staff accounts | Email address<br>Filestore access | Authorised users are able to request this type of account, but must have a valid business case for doing so and follow the relevant procedures for authorisation. Such accounts will be short term and the expiry date (maximum of one year) will be managed in line with the business requirement for creation of the account.<br>The Service Desk within IT Services manually creates this type of account. |
| Generic account | Email Address<br>Filestore access | This type of account is only created if there is a valid business case (see below). The account is not linked to an individual user but linked to a group of users or a role.<br>An example for this type of role is reception@lboro.<br>The Service Desk within IT Services manually creates this type of account. |
| ZZ account | Email Address | This type of account is primary used for short course or conference attendees who require very short-term access and will be created as a student account. These accounts have fixed expiry dates. |
| -ptn | No services offered | This type of account is created for partner organisations based on campus such as Sport Park tenants.<br>User accounts are created in ARMS, which is used to manage all partner organizations. From this, ARMs accounts are automatically replicated within the directory service, managed by IT Services. |
| Athens | No services offered | All staff and students have Athens accounts for access to on-line Library services. These are automatically created at the same time as the individual's main personal account. |

Loughborough University

Information Security

# IT Operations Management

Approved
June 2016

# IT Operations Management

## 1. Policy Overview

The University makes extensive use of computer and information systems for handling and processing information to support its business functions. It is the policy of the University that the systems it uses, and the information it manages, shall be appropriately secured.

This document contains the following policies to ensure that the underlying network and information systems, which use this network, are secure:

- Operations Management;
- Network Management;
- Systems Management;
- Vulnerability Management;
- Software Management;
- Encryption (Cryptography).

## 2. Policy Audience

This policy document contains technical details on how to manage a secure IT environment and is primary aimed at IT Service professionals across the University, including those physically within Schools.

## 3. Operations Management

### Purpose

This section outlines the requirements for the implementation and maintenance of a secure and resilient operational environment.

This sub policy applies to all computers and communications devices owned or operated by the University and any computer or communications devices that are present on the campus network.

### Policy

Physical threats to security include:

- Environmental threats – temperature, humidity, fires, floods, storms;
- System threats – disruption to energy supply, communications;
- Human threats – unauthorised access, tampering, theft, willful damage, accidents.

If buildings are being modified or essential maintenance work is being undertaken, the risks that construction work may present to information systems they house must be addressed and managed in collaboration with Facilities Management.

Data centre areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Staff which are authorised to enter such areas are to be provided with information on the potential security risks and the measures used to control them.

The procedures for the operation and administration of all systems and activities forming part of or related to the University's information systems must be documented by those responsible for them, these procedures and documents shall be reviewed at appropriate intervals.

Changes to operational procedures must be controlled to ensure on going compliance with the requirements of information security and must have management approval.

Duties and areas of responsibility shall be appropriately segregated to reduce the risk and consequential impact of information security incidents that might results in financial or other material damage to the University.

Development and testing facilities for business critical systems shall be logically separate from operational facilities and the migration of change from development to operational status shall be subject to IT Services change process.

Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the systems carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of data are in place.

Procedures shall be established to control the development and deployment of all operational systems.

Reporting of IT security incidents and suspected weaknesses in the University's business systems, should be reported to IT Service Desk either via email it.services@lboro.ac.uk or by calling 01509 222 333.

## High Value Security Risk Areas

Where a room contains core-networking equipment, such as core routers (not regular communication locations which only contain edge switching), only authorised IT Services staff should have access, and should not be shared with School, partner or tenants IT equipment.

Rooms which hold high value and sensitive communications equipment (network core devices and where data is at rest) should meet the following specification:

- Masonry walls or studding reinforced with steel mesh;
- Metal door and frame to insurance LPS-1175 standard:
  - If internal door with an alarm on level 1;
  - f external door with no alarm on level 2;
  - If external door with no alarm on level 3;
- High security lock cylinder;
- Metal security bars to any windows;
- Shelf for visitor log book;
- Cooling to match communications equipment load;
- Proximity card access with PIN keypad;

- Sounder if door is left open;
- Electronic door lock;
- Security alarm Honeywell Galaxy panel (or equivalent);
- Intruder PIR movement detectors;
- Trembler alarms on walls;
- Bold alarm interface unit (or equivalent);
- CCTV covering external view of the door;
- CCTV covering internal view of the door;
- PIR control of lighting;
- IT cabinets with lockable doors (where possible);
- High security cabinet chains (if appropriate).

## 4. Network Management

### Purpose

The University network is a fundamental service that provides interconnects between all of the University's computing resources. It is vital that such a resource is properly controlled, maintained and managed. The purpose of this section covers the management, operation and use of the University data network.

This sub policy refers to the University network managed by IT Services, including the wireless network. The University network covers all building on the campus including student halls of residence (Hallnet) and remote locations such as Loughborough University London. Also covered is the protection of networked services to ensure that users who access the network and networked services do not compromise the security of these services.

### Management

The Network and Communications team within IT Services is responsible for the University's campus network.

The University network shall be managed by suitably authorised and qualified staff to oversee its day-to-day running and to preserve its security and integrity. All network management staff shall be given relevant training in information security.

Other IT Specialists may undertake network moves if the Networks and Communication team has provided relevant training and an agreement is in place.

Switch based reconfigurations of a users' network will only be carried out by staff from the Networks and Communications Team within IT Services.

The implementation of new equipment or upgrades to network software or firmware must be carefully planned tested and managed. The Change Advisory Board must approve any changes.

AAA (triple A) (authentication, authorisation and accounting) methodology must be implemented on network devices wherever possible using technologies such as RADIUS and TACAS+.

Where there is a risk of the network security, quality of service for network users, or in order to enforce University policy, IT Services is authorised to:

- Impose restrictions on network traffic or use of network applications;
- Refuse connection of devices to the network;

- Remove networked devices or sub-sections of the network from service;
- Manage network resource allocation (e.g. bandwidth).

## Monitoring

Network appliances or devices, which are critical to providing networking services to end-users must be monitored to ensure they are performing as expected.

Servers managed by the Networks and Communications Team, which provide network related services must be monitored to ensure the services are performing as expected.

Where the status of a monitored appliance, device, server or service changes to be critical an automated email alert must be sent to the Networks and Communications Team.

For the purpose of monitoring bandwidth across the campus network, links to and from park routers will be monitored, graphed and reviewed on a regular basis.

All servers centrally managed by IT Services providing services must be backed up using the backup solution provided by IT Services.

Where other IT Specialists manage servers, it is the responsibility of the service manager to ensure appropriate backups are taken at regular intervals.

All network appliances and devices must be able to back up their configuration to a central location, which must be maintained for a minimum of seven days.

Logging from network appliances and devices must be forwarded to a central location and stored for a minimum of thirty days.

## Network design and configuration

The network must be designed and configured to deliver levels of performance, security and reliability suitable for the University's business needs, whilst providing a high degree of control over access.

The network should be segregated where appropriate into separate logical sub-networks taking into account security requirements, with routing and access control lists operating between the sub-networks. Appropriately configured firewalls and other security mechanisms where appropriate shall be used to protect the sub-networks supporting the University's business critical systems.

Local area networks (LANs) in individual buildings, or extensions to them should only be designed and installed by IT Services.

IT Services is responsible for providing the enterprise wireless network service. Schools or Professional Services are prohibited from establishing their own wireless network and adding wireless access points unless authorised to do so by the Networks and Communication Team. This is to ensure the security, integrity and resilience of the wireless service is maintained.

IT Services reserve the right to make changes to network security as and when necessary. This may be in relation to a security threat or to improve existing arrangements.

Formal change control procedures, with a full audit trail, shall be used for all changes made to the University network infrastructure. All such changes must be risk assessed and authorised by the relevant manager before being making configuration changes.

## Security and resilience

Reasonable measures based on a risk assessment, such as fire and water protection, locked dedicated space, secure cabinets etc, must be taken to protect networks and communication equipment against accidental damage, security breaches, theft or malicious intent.

The network should where possible incorporate logical and physical resilience features to help mitigate against the impact of failure or physical damage to cabling and other network equipment.

## Network services and protocols

Only IT Services will manage the IP address space, which has been allocated to the University and operate Dynamic Host Configuration Protocol (DHCP) service to issue IP addresses.

IP address blocks allocated to schools will be managed my local IT support staff using the “Hostbuilder” tool provided by IT Services.

The Networks and Communications Team within IT Services manages IP routing protocols running on the University’s core routers. Routing protocols such as EIGRP, OSPF, ISIS should be disabled when commissioning IP capable devices.

The use of network management tools such as SNMP is restricted to IT Services staff, unless requests have been approved.

University servers running Domain Name Service (DNS) are managed and maintained by the Networks and Communications Team within IT Services.

University servers running Dynamic Host Configuration Protocol (DHCP) are managed and maintained by the Networks and Communications Team within IT Services.

University servers running Network Time Protocol (NTP) are managed and maintained by the Networks and Communications Team within IT Services

University servers running RADIUS and TACACS+ are managed and maintained by the Networks and Communications Team within IT Services.

## Management interface access

Network appliances and devices shall not expose any management interfaces via the Internet. All management interfaces shall have the appropriate restrictions applied so access is only granted via privileged networks.

Remote access to devices connected to the University’s network is permitted via Off-campus Working (Virtual Private Network).

Only Remote Desktop Protocol (RDP), Virtual Network Computing (VNC) and Secure Shell (SSH) is permitted through the Virtual Private Network as standard. If other protocols are required for management and/or service delivery, please contact IT Services to discuss your requirements.

## Incidents and emergency procedures

Any incident or emergency relating to the University’s network should be reported to the Service Desk in IT Services.

IT Services must ensure that prompt and effective action is taken in response to requests and information from JANET CSIRT (Computer Security and Incident Response Team).

## 5. System Management

### Purpose

The University's information systems are a fundamental resource for the University and its business. It is vital that such a resource is properly controlled, maintained and managed. This section covers the management, operation and use of University Information Systems.

This sub policy covers all computers owned or operated by Loughborough University and any computers that are present on the campus network which are connected under the agreed Business and Community Engagement Jisc Policies.

### Policy

The University's Information Systems shall be managed by suitably trained and qualified staff to oversee their day to day running and to preserve data security, confidentiality and integrity.

All systems management staff shall be given relevant training in information security and sufficient training to securely operate the systems they are required to manage.

Technical Service Owners or individuals responsible for Information Systems are to maintain the appropriate access controls for their systems and keep records of any elevated access they give out to other users.

Technical Service Owners or individuals responsible for Information Systems are responsible for correct and secure operation of computers in accordance with related University policies.

Access to all Information Systems, excluding publicly accessible data sources, shall use a secure authentication process. Consideration should also be given as to whether it is appropriate and feasible to further limit the access to business critical systems by time of day, the location of the access, or by an automatic timeout following a defined period of inactivity. Access to information systems is to be logged and monitored where appropriate to identify potential misuse of systems or information

Information Owners, Technical Service Owners and individuals responsible for the Information Systems must ensure that appropriate backup and system recover procedures are in place, dependent upon the accessed level of criticality of the information concerned. Backup of the University's information systems and critical assets and the ability to recover then is an important priority.

Business Service Owners are responsible for ensuring that the University's information systems and critical data is frequently backed up and procedures for recovery meet the needs of the business.

Passwords for the systems should adhere to the University password policy: www.lboro.ac.uk/services/it/reg/guidance/

Storage of passwords should be carried out in accordance with a well defined password storage policy.

Only authorised staff will be permitted to perform systems administration or management functions. Use of commands to perform these functions should be logged and monitored where it is considered appropriate and feasible to do so.

Formal change control procedures, with audit trails, shall be used for all changes to business critical systems. All such changes must be risk assessed and authorised by the IT Services Change Advisory Board or relevant manager before being moved to the live environment

Security event logs, operational audit logs and error logs must be reviewed and managed by qualified staff.

System clocks should all be synchronised to the Universities NTP server. In the case of computers in the Active Directory this will happen automatically.

# 6. Vulnerability Management

## Purpose

The purpose of this section is to allow IT Services within Loughborough University to scan devices attached to the university network for vulnerabilities. This is to assist in maintaining a secure and reliable infrastructure.

Vulnerability scanning may be conducted to:

- Identify compromised systems within the campus network;
- Identify virus infected machines within the campus network;
- Identify poorly configured and potentially vulnerable systems attached to the campus network;
- Any device requesting a firewall rule;
- Investigate possible security incidents to ensure systems conform to Loughborough University's security policies.

This sub policy covers all computers and communications devices owned or operated by Loughborough University and any computers or communications devices that are present on the campus network which are connected with agreed Business and Community Engagement Jisc terms. This is highlighted in the University AUP.

## Scanning

Loughborough University IT Services will use security-scanning software to conduct vulnerability scanning and audit reports.

A number of tools will be used for vulnerability scanning and the tool set will be reviewed annually. This includes: Open Source, commercial packages and services provided by ESISS (Education Shared Information Security Service).

These tools will perform the following tasks:

- Host Discovery – identifying computers listening on the campus network;
- Port Scanning;
- Operating System Detection – remotely determine the OS (Windows, Apple Macintosh or Linux);
- Software Version Detection – Interrogating listening services to determine application names and versions;
- Network based vulnerability scanning;

- Operating systems security patch audits (Windows, Linux);
- Configuration audit;
- Web application vulnerability testing;
- SQL database vulnerability and configuration auditing;
- Password auditing, checking for default or blank passwords;
- Anti Virus audit, checking out-of-date virus signatures and configuration errors.

## Policy

In an effort to reduce IT Security risks and supplement existing security practices, IT Services will perform periodic vulnerability audits on devices connected to the campus network.

IT Services may also scan for vulnerabilities, which are currently being exploited in the wild.

Vulnerability audits will consist of campus network scans for:

- Open communications ports;
- Host operating system detection;
- Host operating system patch levels;
- Remote applications to identify known vulnerabilities or high-risk system weaknesses.

Any new systems or services should have passed a vulnerability scan before being connected to the production network.

Any systems or services, which require off-campus access, are subject to a vulnerability scan before access is granted. This is to ensure that the hosts posture is adequate.

All systems or services which currently have off-campus access enabled are subject to vulnerability scanning every six months.

Any systems or services that require access via the VPN service or Remote Working Portal are subject to passing a vulnerability scan.

Before IT Services carry out any vulnerability scans; server managers should be contacted to arrange a suitable time.

Vulnerability scanning will not search the contents of personal electronic files located on the system.

Scans should not cause disruption to the campus network or services hosted on systems being scanned. Device log files may reflect the scan that takes place.

Servers hosted within IT Services datacentres, will be subject to a three monthly automated authenticated security scan; and as such will require the service account Lunet\secscan-svc to have local administrator permissions. If a software firewall is installed, a hole will be required to the scanning server’s IP address.

Servers not hosted within IT Services datacenters, but have services exposed to the Internet are subject to a three monthly automated security scan.

## Managing Vulnerabilities

Vulnerabilities identified against hosts will be emailed to the Technical Service Owners or individuals responsible for the Information Systems.

Technical Service Owners or individuals responsible for the information systems are responsible for ensuring the identified vulnerabilities are remediated in a timely manner, typically one calendar month, but dependant on a risk assessment).

**Vulnerability remediation matrix**

| **Information Category** | Critical Vulnerability | High risk vulnerability | Medium risk vulnerability | Low risk vulnerability |
|---|---|---|---|---|
| Highly confidential | **Remediate** | **Remediate** | **Remediate** | **Remediate** |
| Confidential | **Remediate** | **Remediate** | **Remediate** | **Recommended** |
| Not Sensitive / Public | **Remediate** | **Remediate** | **Recommended** | **Recommended** |

The Network and Communications team will be made aware of vulnerabilities which have been identified and the issue not been resolved by the Technical Service Owner or individuals responsible for the information system.

If identified vulnerabilities are unable to be resolved, steps must be taken by the Technical Service Owner or individuals responsible for the information systems to mitigate the risk of exposure and ensure the risk is recorded and accepted.

Failure to remediate identified vulnerabilities within a suitable timeframe, typically one calendar month, may results in firewall rules being removed or removing the network connection from the server. This is to ensure that the security and integrity of the network is not compromised for other information systems and the users of the network.

## 7. Software Management

IT Colleagues should be fully aware and compliant with the University Software Policy:

http://www.lboro.ac.uk/services/it/about/policies/software/

# 8. Encryption (Cryptography)

## Purpose

This section sets out principles and expectations about when and how encryption of University digital information should (or should not) be used and applies to the following:

- Managers who are responsible for the provision of information systems;
- Staff and students of the University who handle sensitive information through employment or study;
- Third parties who handle sensitive information on behalf of the University.

## Use of encryption

Loss, theft, or unauthorised disclosure of sensitive information could be detrimental to the University, its staff or students. Such information includes personal data defined by the Data Protection Act 1998. Where the University is handling digital personal data that cannot be secured by physical controls, the data must be encrypted.

Data, which must be handled securely, using encryption includes:

- Any personal data classed as “sensitive” by the Data Protection Act;
- Any data, that is not in the public domain, about a significant number of identifiable individuals;
- Personal data in any quantity where its protection is justified because of the nature of the individuals, source of the information, or extent of the information;
- Data classified as Confidential or Highly Confidential by the University Information Classification policy.

Data described above must be encrypted:

- When stored on a computing device or any computer storage which may be exposed to a significant risk of being lost or stolen. Any device when outside a secure University location should be considered to be at risk, including home computers;
- Where it is to be transmitted via a computer network using mechanisms that do not itself incorporate encryption. This could refer to: sending data by email either within or outside the organisation, transferring files offsite, remotely accessing files or web pages;
- Where the data is being sent using a postal service such that the data media could be lost, stolen or intercepted and read whilst in transit.

Data being handled by the University is subject to an agreement with an external organisation specifying the use of encryption.

Personal data is to be encrypted and no overriding requirements (from external body) apply, the recommended minimum University standards (or better) must be applied.

University web transactions that involve the transfer of sensitive data or funds must use encryption, e.g. use of HTTPS.

## Management of encryption keys

Procedures must be in place:

- To manage encryption keys in a way that ensures encrypted stored data will neither become unrecoverable nor accessible by an unauthorised person;

- To facilitate authorised persons of the University to obtain prompt access to the encrypted information in the case of an emergency or investigation;
- To ensure that encryption keys are stored and always communicated securely;
- To record who holds encryption keys relating to important information;
- To revoke encryption keys when key holders leave.

Where practical, an unencrypted backup copy of critical University data should be securely maintained. Critical backup data should be stored where there is appropriate physical security.

## Unsupported use of encryption

Staff and students should:

- Not store encrypted data on University systems except where they are able to justify doing so for legitimate purposes;
- Be aware that the University reserves the right to request site, at any time, of the unencrypted version of any data stored on its systems and the option to remove any data.

## Cryptography implementation

All encryption products, standards and procedures used to protect sensitive University data must be ones which have received a public review and have been proven to work effectively. Any product used must be certified to FIPS 140-2.

Where a School or Professional Service elects to undertake an activity that would incur a cost, in order to remain compliant with the University Information Security Policy, then that cost should be highlighted at ITGC.

Loughborough
University

Information Security

# Management of Information Security Incidents and Review of Policies

Approved
June 2016

# Management of Information Security Incidents and Review of Policies

## 1. Purpose

The Information Governance Policy (link) commits the University to investigating and monitoring all reported instances of actual or potential breaches of confidentiality and information security. The aim of investigation and monitoring is to minimise the risk of data loss to members of the University and the public, and, at the same time, manage any potential reputational damage to the University.

When handling information security incidents, the University will ensure that:

- Incidents are reported and investigated in a timely manner and by the appropriate staff member or staff members.
- Incidents are logged and documented.
- Incidents are reported to external bodies and data subjects as and when it is appropriate to do so.
- Incidents are handled in accordance with all appropriate legislation, and in particular the Data Protection Act (1998).
- Investigations are undertaken in a fair and open manner.
- Incidents are reviewed to identify potential improvements to working practices and amendments to relevant policies.

As outlined in the Roles and Responsibilities for All Staff and Research Students Policy and the AUP, individuals will be expected to report all incidents and suspected incidents to the appropriate staff member (see below) or, alternatively, email abuse@lboro.ac.uk.

The Chief Operating Officer is the senior officer responsible for information governance and ensuring that all information security incidents are handled in a manner which ensures compliance with the relevant legislation.

## 2. Scope

This policy is relevant to all staff, students, external partners and the public.

## 3. Information Security Incident Handling

Once identified, all information security incidents and suspected incidents should be reported to the individual’s line manager, or supervisor, in the first instance. Where there is any doubt about to whom the incident should be reported, Information Security staff in the Academic Registry should be approached for guidance.

The person to whom the incident has been reported must take any necessary steps to contain the incident, and, following this, escalate the incident to the appropriate member of Information Security staff in the Academic Registry.

Where appropriate, Information Security staff will engage with the relevant stakeholders and undertake an investigation of the incident in order to establish;

- The cause of the incident.
- The extent to which information may have been placed at risk.
- The potential damage that may have been caused to data subjects and/or any reputational damage that may have been caused to the University as a result of the incident.

Following the investigation; Information Security staff will produce a report and make a recommendation as to any further action that is required following the incident. This should include:

- A recommendation on whether or not to inform the relevant legislative organisation (e.g. Information Commissioner’s Office) of the incident.
- A recommendation on whether or not to inform data subjects of the incident and the corrective measures taken.
- A recommendation on any remedial action that should be taken in order to ensure that the circumstances are not repeated.

The report will be passed to the Academic Registrar for a decision on the action (if any) that should be taken. In serious cases, the Academic Registrar will make a decision in consultation with the Chief Operating Officer.

Following the review of an incident it may be necessary for further training to be undertaken by staff members from within those areas that are deemed to be at risk. Where there is evidence of wilful negligence or deliberate intent in the inappropriate release of information, it may be necessary to consider disciplinary action, as outlined in the Responsibilities of All Staff and Research Students Policy and the Acceptable Use Policy. Any such action would be taken in accordance with the procedures set out in the relevant Ordinances on discipline for staff and students.

www.lboro.ac.uk/governance/ordinances/35/current/ (staff)

www.lboro.ac.uk/governance/ordinances/17/current/ (students)

## 4. Monitoring of Information Security Incidents

All recorded information security incidents will be detailed for full consideration by the Information Governance Sub Committee (anonymised as far as possible). The Sub Committee will identify any recurring incidents or areas of risk and will make recommendations for possible additions or amendments to the existing policies and/or training.

A report detailing all recorded information security incidents and recommendations for remedial actions will be submitted to the Information Technology Governance Committee on an annual basis. An immediate report will be made should an incident of high concern arise. Any proposed changes to policies will be considered by the Information Technology and Governance Committee and recommended to Senate and Council for approval.

## 5. Review of Information Security Policies

All Information Security policies, and the associated framework, will be reviewed on a regular basis by the Information Governance Sub-Committee, to ensure that they remain relevant, up to date and fit for purpose. Revisions to policies will be considered initially by the Information Technology and Governance Committee as noted above.