Integrated
Research Campus

UNIVERSITY OF LEEDS

Framework of the Information Security Management System

Version 1.0

Version Date 20/10/2016

Document Information

Reference	IRC ISMS F
Category	ISMS Documents
Title	IRC Framework of the Information Security Management System
Purpose	Framework on information security in the IRC
Version	1.0
Status	Approved, External
Owner	IRC Information Governance Management Group
Author	Samantha Crossfield
Compliance	ISO 27001 for scope defined herein
Review plan	Set in the IRC IS Documentation Procedure
Related Documents	University of Leeds Information Protection Policy IRC Information Governance and Security Policy

Version History

Version	Date	Change description
0.1	27/06/2016	Initial version
1.0	20/10/2016	Submitted for sign off

Sign-Off

Name	Date	Role
Barry Haynes		Chair of IGMG and Head of Enterprise Architecture, University of Leeds

Master version:
Signature……………………………………………

Table of Contents

1. Purpose

The Integrated Research Campus (IRC) is a University of Leeds Central IT provision. It provides secure technical infrastructure and services for research data handling, analytics, application processing and development. This document is part of the IRC information security management system (ISMS).

This document defines the goal, context and scope of the IRC ISMS. It defines the ISMS objectives and requirements for information security. The purpose of this is to set the information security framework for IRC operations and management in support of the University's Information Protection Policy and other relevant security policies.

All ISMS documentation terms are defined in the **IRC Glossary of Terms**.

2. Applicability

This framework sets out the ISMS that applies to users and providers of IRC services and infrastructure. This is regulated and contracted as outlined in Section 8). It is for use by, and is provided (in electronic or paper format) to:

1. Employees and contractors providing IRC infrastructure and services
2. Users of IRC resources
3. The IRC Information Governance (IG) Management Group
4. Auditors of the IRC ISMS and individual standard operating procedures
5. Others reading the IRC operating procedures

3. The IRC Information Security Management System

The IRC ISMS sets information security (IS) as a key element of the mission statement of the IRC. It is designed to protect IRC reputation and capacity by maximising IS throughout the data lifecycle. It aims to ensure the appropriate management, control and treatment of risks to preserve the confidentiality, integrity and availability of information.

This document sets the framework for meeting this goal. The ISMS context has been set in Section 4 to meet the data handling needs of data subjects, data providers and users. The ISMS scope is defined in Section 5 and the procedures to manage, improve and uphold the ISMS are set out in Section 8. Section 11 sets the IS objectives that are designed to meet the ISMS aim. The documentation and requirements listed in Sections 8 and 9 determine how the IRC may deliver its services to ensure that the ISMS aim is met.

An aim for the IRC ISMS is certification to ISO / IEC 27001:2013 and the NHS Digital IG Toolkit Level 3[1, 2]. This will externally validate that IS best practice has been adopted within the scope defined in Section 5.

4. Context

4.1 Opportunities

There are increasing opportunities for data analytics that transforms practice. There is unprecedented growth in the scale of data capture, data variety (in structure, content and reliability) and opportunities for linkage. Data being captured includes geographic, socio-economic, consumer, social, clinical and '-omics' information. Such data may be person- or place-level specific or aggregated to relate to an area or group. It may be in de-identified format or collected in line with legal requirements. New computational and analytical methods are required to transform such data into new understanding that inspires meaningful change.

4.2 Requirements

This increasing data diversity raises differing requirements for data handling in terms of information security, governance and data protection. New processes for data handling and analysis are essential for ethically deriving insight from data. Research Councils and industry are funding programmes to develop these procedures. In the UK, centres of research, analysis and training are leading the development of the capacity for data utilisation. One such centre is the Leeds Institute for Data Analytics, LIDA. It draws together research groups and data scientists with external partners to undertake data-intensive research.

Given the requirements associated with data, such programmes depend on secure data services that meet information governance standards. To meet this goal means using secure infrastructure for research data handling by the right people in the right way.

[1] NHS Digital Information Governance Toolkit: https://www.igt.hscic.gov.uk/
[2] ISO/IEC 27001:2013 - http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

4.3 Summary

The Integrated Research Campus (IRC) provides data-intensive organisations such as LIDA with the infrastructure, training and data services required for secure data handling in research.

The IRC is a University of Leeds IT platform and is both shaped by and contributes to the University's strategy, research objectives, operational processes and management structures.

To meet the ISMS aim, the IRC's data handling processes have been developed in line with information governance gold standards, such as those applied for the protection of payment card data. Its operations are designed to prevent and minimise security incidents. This principally avoids unauthorised disclosure that could lead to industrial or personal investigation and loss of reputation.

The processes delivered are summarised as:

- Data capture, review and release (gateway) services
- Data storage facilities
- Data processing services including data cleansing, transform, linkage, de-identification, backup and destruction
- Monitored, regulated access to data in a Virtual Research Environment (VRE)

Figure 1 shows the main services groups and lists some example services.

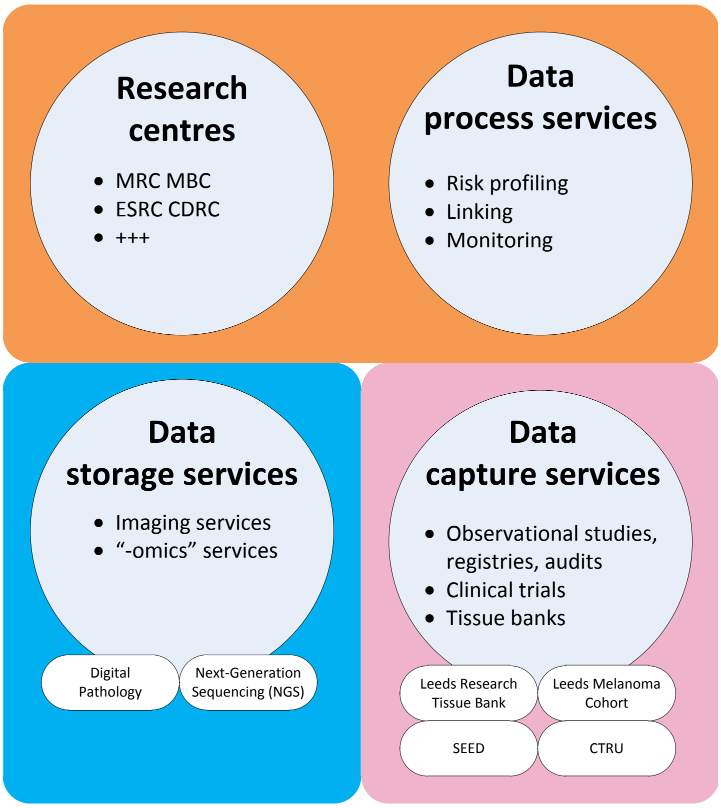

Figure 1: Main services and centres that utilise the IRC

5. Scope

The ISMS scope encapsulates the space that meets the organisation's needs for secure data handling. This corresponds to the reach of the IRC secure research environment and the services conducted therein, regardless of location, provider or user.
Figure 2 summarises the scope and the governance structure that it resides in.

The ISMS objectives apply to all in-scope elements. There is mandatory compliance with the ISMS within this scope. Exceptions must be handled as set out in the IRC IS Audit and Management Procedure.

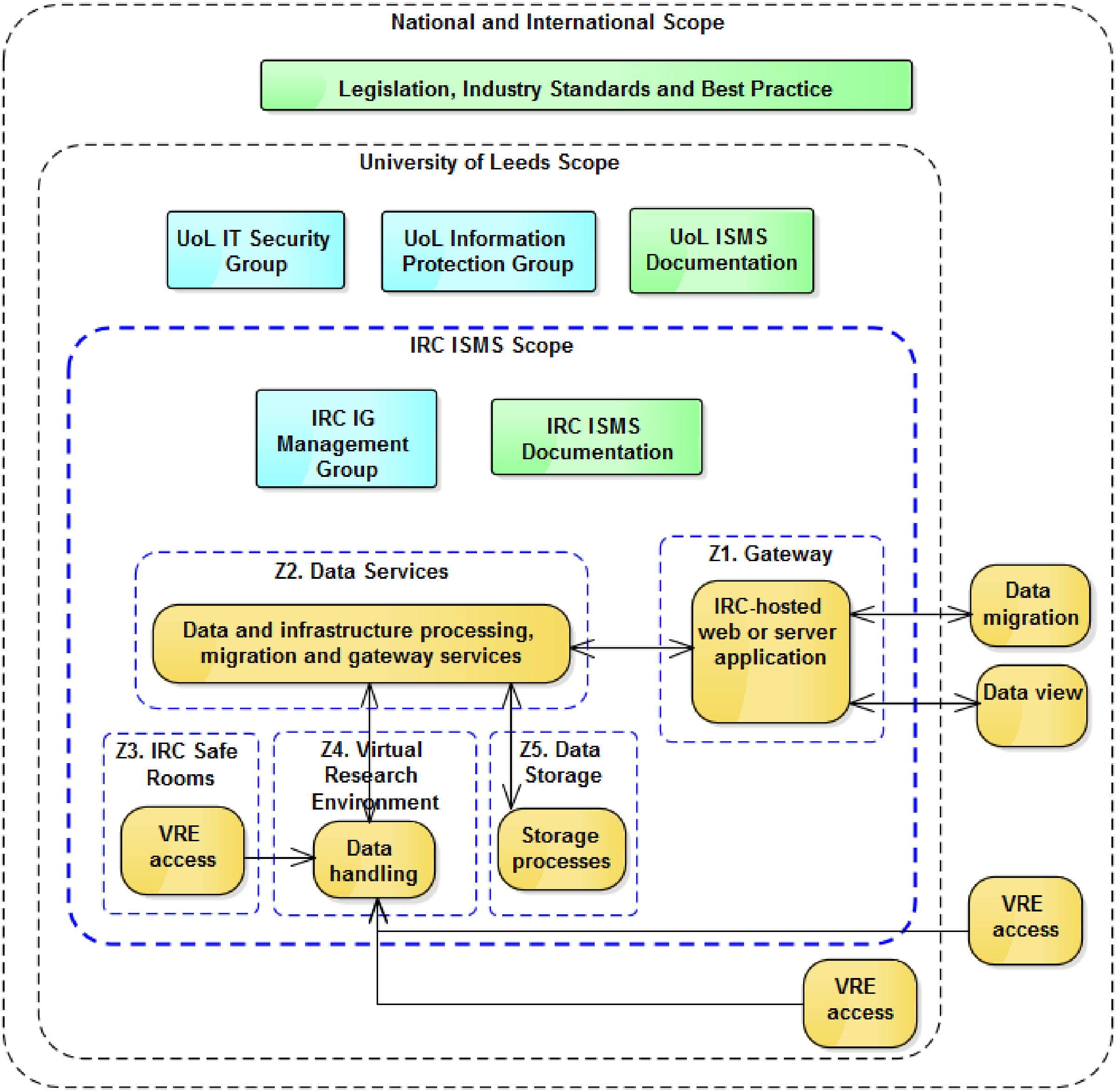

Figure 2: Representation of the IRC Services (yellow), Governanace (blue) and Processes (green) .

Figure 2 shows the IRC ISMS scope and how it fits under the scope of the University and wider legislation and standards. The ISMS scope is defined by the blue dashed line.

5.1 Zones

IRC zones are numbered 1-5 in **Figure 2**:

1. IRC Gateway – the gateway zone between the other IRC zones and the external environment. Data passes through here in order to move between zones or to

enter or leave the IRC

2. IRC Data Services – core data services are provided from this zone to users, including access, provisioning, management and support services

3. IRC Safe Rooms - secure and managed rooms providing monitored access to data

4. IRC Virtual Research Environment (VRE) – firewalled virtual machines that are set up for users with appropriate software, applications and data access. VREs are remotely accessed

5. IRC Data Storage – the zone in which research data is securely stored

5.2 Infrastructure

*We define In Scope in **Figure 2**:*

1. Infrastructure in the IRC Gateway (Zone 1). This includes:
    a. Interfaces, such as an SFTP or Web server for uploading data
    b. External facilities used in providing secure IRC data services where they are brought in scope by either a:
        i. Formal agreement *or*
        ii. 'Take-over' of facilities as set out in the IRC Policy on Data Transfer
2. Infrastructure in the IRC Data Services (Zone 2)
3. Infrastructure in the IRC Safe Rooms (Zone 3), including thin client computers
4. Infrastructure in the IRC Virtual Research Environment (VRE) (Zone 4), including the software and applications in each virtual machine
5. Infrastructure in the IRC Data Storage Zone, used to deliver storage services
6. Networking / Telephony Systems supporting Zones 1 to 5

The above (1-6) are hereon referred to in all ISMS documentation as the "IRC infrastructure".

We define Out of Scope:

1. Systems that receive data from the IRC, such as external high performance computing or web applications
2. Programmes and devices used to capture data relayed to IRC infrastructure. This includes scanners, gene sequencers, websites and application
3. Devices used to access the IRC infrastructure (including desktops, laptops, tablets and smart phones) and their locations

5.3 People

In Scope:
1. Members of the IRC Data Services Team (based in Zone 2)
2. Users such as researchers, clinicians and analysts while they are using a) the IRC infrastructure or b) an application that calls upon the IRC infrastructure. A user agreement must define the elements of the ISMS that pertain to the user
3. IT and support staff and contractors working on the IRC infrastructure. Contracts, service and operating level agreements must accord with the ISMS
4. Suppliers and data providers who enter a contractual agreement with the IRC. The agreement of what is supplied and how must be in line with the ISMS

Out of Scope:
Users, IT and support staff and data providers while they are not interacting with IRC infrastructure.

Where actions lead a person across a regional boundary the governance structures within all crossed regions apply. For example, the IRC ISMS and University of Leeds policies apply to a research group while they are logged in to the VRE (
Figure 2).

5.4 Services

In Scope:
Services delivered on IRC infrastructure. This can be summarised as data capture, process, access and storage services, including:
1. Checking and loading of data to / from the IRC Gateway infrastructure. This must be in line with data agreements
2. Development and destruction of virtual machines and access rights
3. Data transformation, linkage and management
4. Data visualisation and presentation
5. Auditing of the use of IRC infrastructure
6. Data capture services that reside on IRC infrastructure

5.5 Information assets

In Scope:
Data held on IRC infrastructure – from entry to exit via the IRC Gateway or until deletion.

Out of Scope:
Data held beyond the scope of the IRC infrastructure.

6. Scope Interplay

Projects usually involve movement of data in and out of scope of the IRC ISMS and transfer must be handled according to the IRC Policy on Data Transfer.

7. Information Security Objectives

The IRC Objectives have been set to address the ISMS aim and are based on the ISO 27000 Series of documents.
Table 1 lists the objectives and the controls that have been documented in order to ensure they are met by everything within the ISMS scope. They were developed and adapted in response to external and internal issues that may affect the ISMS aim.

The objectives and controls cover the following:

- Measurable where practicable *(all IRC ISMS documentation)*
- Procedures to account for IS requirements and outcomes from the risk assessment and risk treatment plan *(IRC Risk Assessment Procedure, IRC IS Audit and Management Procedure)*
- Define how they are planned, communicated, controlled and updated *(IRC Documentation Procedure, IRC IG Training Procedure, IRC IS Audit and Management Procedure)*
- An outline for achievement: steps, resources, responsibilities, timeframe, evaluation *(all IRC ISMS documentation)*
- Audited documentation of achievement *(all IRC ISMS documentation)*
- A process for reviewing changes to information-handling and taking action to mitigate any adverse effects *(IRC IS Audit and Management Procedure)*
- A process to define and control outsourced work *(IRC Access and Usage Policy)*

Table 1: IS Objectives and their corresponding ISMS controls

Objective	Detail	Control
To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	Policies for information security	1. IRC Information Governance and Security Policy 2. IRC Framework of the Information Security Management System
	Review of the policies for information security	IRC IS Audit and Management Procedure
To establish a management framework to initiate and control the implementation and operation of information security within the organisation	Information security roles and responsibilities and their segregation	IRC IS Audit and Management Procedure
	Contact with authorities and ethics organisations	IRC IS Audit and Management Procedure
	Information security	IRC IS Audit and Management Procedure

	in project management	
To ensure the security of teleworking and use of mobile devices.	Mobile device and teleworking protocols	IRC Access and Usage Policy IRC User Agreement
To ensure that employees and contractors understand their responsibilities and are suitable for their roles.	Screening and service conditions	1. University of Leeds Recruitment Framework 2. Service Level Agreement between the University of Leeds and the third party 3. IRC Access and Usage Policy
To ensure that employees and contractors are aware of and fulfil their information security responsibilities.	Management responsibilities	IRC IS Audit and Management Procedure
	Information security awareness, education and training	IRC IS Audit and Management Procedure
	Disciplinary process	IRC Framework of the Information Security Management System
To protect the organization's interests as part of the process of changing or terminating employment.	Termination or change of employment responsibilities	IRC Framework of the Information Security Management System
To identify organizational assets and define appropriate protection responsibilities.	Inventory, ownership, use and return of assets	1. IRC IS Audit and Management Procedure 2. IRC Risk Assessment Procedure 3. IRC Access and Usage Policy 4. IRC User Agreement
To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.	Classification and labelling	1. IRC Data Classification Procedure 2. IRC Data Handling Summary
	Asset handling	1. IRC IT Environment and Infrastructure Procedure 2. IRC Data Handling Summary 3. Service Level Agreement between the University of Leeds and the third party 4. IRC User Agreements
To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	Management of removable media, media disposal and transfer	1. IRC Storage, Archiving and Destruction Procedure 2. IRC Access and Usage Policy 3. IRC Data Transfer Procedure 4. IRC User Agreement
To limit access to information and information processing facilities	Access control policy, including network access	1. IRC Access and Usage Policy 2. IRC IT Environment and Infrastructure Procedure 3. IRC HPC Procedure
To ensure authorized user access and to prevent unauthorized access to systems and services.	Management and review / amendment of registration, authentication and access provision	1. IRC Access and Usage Policy 2. IRC User Agreement
To make users accountable for safeguarding their authentication information.	Use of secret authentication information	1. IRC Access and Usage Policy 2. IRC IS Training Procedure 3. IRC User Agreement
To prevent unauthorized access to systems and applications	Access restriction procedures and password management	1. IRC Access and Usage Policy 2. IRC User Agreement 3. IRC IT Environment and Infrastructure Procedure 4. IRC Virus Protection and Management Procedure 5. IRC IT Programming Procedure

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information	Use of cryptographic controls and key management	1. IRC IT Environment and Infrastructure Procedure 2. IRC IS Training Procedure
To ensure physical and environmental security	Secure areas and equipment for uninterrupted and authorised operations	1. IRC IT Environment and Infrastructure Procedure 2. IRC Virus Protection and Management Procedure 3. IRC Access and Usage Procedure~~olicy~~
To ensure correct and secure operations of information processing facilities	Operating procedures and controlled change management. Controls against malware	The IRC SOPs, particularly: 1. IT Environment and Infrastructure 2. Virus Protection and Management 3. Access and Usage Procedure
To ensure the integrity and auditing of systems, and prevent data loss or exploitation of facilities	Information backup, logging, clock synchronisation, controlled installation and management of technical vulnerabilities	The IRC SOPs, particularly: 1. IT Environment and Infrastructure 2. Virus Protection and Management 3. Access and Usage 4. Documentation and Control 5. Audit and Management Review 6. Development and Deployment
To ensure security of information in networks and transfer	Network control, security and segregation, and transfer standards	1. IRC IT Environment and Infrastructure Procedure 2. IRC Access and Usage Procedure 3. IRC Data Transfer Procedure
To ensure information security throughout the lifecycle of system development and maintenance	System requirements, secure development policy, test data and environment	1. IRC IT Programming Procedure 2. IRC IT Environment and Infrastructure Procedure 3. Supplier Service Agreement 4. IRC IS Communications Procedure 5. IRC Project Risk Assessment
To ensure security in supplier relationships	Supplier agreements and monitoring	1. Supplier Service Agreement 2. IRC IS Audit and Management Procedure
To ensure the management of IS incidents and the continuity and improvement of information security	Reporting, assessment and review process; security continuity plan	The IRC ISMS, particularly: 1. Audit and Management Procedure 2. Framework of the Information Security Management System 3. Risk Assessment Procedure 4. Risk Treatment Procedure 5. Event Handling Procedure
To ensure availability of information processing facilities.	Implementation of redundancy	IRC IT Environment and Infrastructure Procedure
Review of IS, and legal and contractual compliance	Application and regulation of required controls and independent review	1. IRC IS Audit and Management Procedure 2. IRC Risk Assessment Procedure

8. Information Security Management and Responsibility

The IRC ISMS is approved by the IRC Information Governance (IG) Management Group. This Group is committed to the continual improvement and applicability of the IRC ISMS. The Group Chair is ultimately responsible for the maintenance of the ISMS and for compliance within the IRC.

The IRC IG Management Group is responsible for reviewing the ISMS on an annual basis and as required. The procedure for review and its triggers are defined in the IRC IS Audit and Management Procedure. The Group directs, supports and promotes information security through appropriate commitment and adequate resourcing.

The **IRC IS Audit and Management Procedure** defines the flow of accountability in the IRC for information security. It sets out the representation and roles in the IRC IG Management Group and their responsibility for the ISMS management and oversight. The Group oversees the IRC Data Services Team that operate the IRC processes. The team ensure that in-scope people (Section 5.3) have relevant training and approval as per the IRC Access and Usage Procedure and IRC IG Training Procedure. This ensures that people are:

- Aware of how the ISMS applies to their role and their responsibilities
- Given appropriate support and resources to comply with the IRC ISMS

The manager on each project that uses IRC resources is responsible for authorising access to any IRC-held information assets.

For University staff and contractors, University policies on fraud, bribery and whistle-blowing apply. Responsibilities for information security remain valid following change of employment. This is set out in the University's policies, procedures and codes of practice and communicated through a University contract.

9. Information Security Risk

Information security risk is assessed and treated in accordance with the IRC Risk Assessment Procedure and IRC Risk Treatment Procedure. The IRC Data Services Team leads these activities with oversight from the IRC IG Management Group as set in the **IRC IS Audit and Management Procedure**. The Group Chair is the Senior Information Risk Owner (SIRO) and takes overall accountability for risk levels, assessment and treatment.

10. Information Security Breaches

All information security incidents and suspected ISMS breaches are reported and investigated as per the IRC Event Handling Procedure. The IRC Data Services Team receive reports and response is overseen by the IRC IG Management Group. Confirmed security breaches trigger the implementation of controls as per the University of Leeds Security Incident and Misuse Policy. Any breaches of personal data will be reported to the University's Data Protection Officer. Records of the number and type of any security breach will be logged indefinitely by the University's IT Security Team.

Failure to comply with the ISMS may result in action being taken in accordance with existing University procedures. This will be triggered and conducted in accordance with the University of Leeds policies, procedures and codes of practice. Non-conformities are addressed in a contained manner subject to audit, review and corrective action. Any resultant change requirements for the ISMS are handled as defined in the IRC IS Audit and Management Procedure.

11. Wider Legislation and Standards

The IRC ISMS procedures and processes must follow legal requirements and best practice for data handling and information security in order to meet the IS objectives (Section 7). This includes incorporating requirements from the following wherever they apply to an aspect that is within the ISMS scope (Section 5):

UK Acts of Parliament and Case Law

- Data Protection Act 1998
- Counter-Terrorism and Security Act 2015
- Freedom of Information Act 2000
- The Common Law of Confidentiality
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988

International Standards

- The ISO/IEC 27000 series of information security management standards

University of Leeds Policies, Procedures and Codes of Practice

- The University of Leeds Information security policies and guidance
  - Including the University of Leeds Information Protection Policy
- The University of Leeds Code of Practice on Data Protection
- The Faculty of Medicine and Health Classified Information Security Policy

Policies and Standards for the use of NHS and Social Care Data

These apply where applicable NHS data is handled on IRC infrastructure

- Confidentiality: NHS Code of Practice
- The Health and Social Care Act 2012

- The NHS Care Record Guarantee for England
- The Social Care Record Guarantee for England
- The Information Security NHS Code of Practice
- The Records Management NHS Code of Practice
- Records Management: NHS Code of Practice
- NHS Act 2006 Section 251 (use of non-consented NHS data)

Appendix 1 provides further information on some of the more widely applicable aspects from this list and relevant controls put in place by the University of Leeds.

Appendix 1

Further information on some of the Acts referenced in Section 11:

A1.1 Data Protection Act 1998

The University of Leeds is registered to process personal data, in particular for the purposes of research. The University is registered formally under the Data Protection Act (DPA); its registration number is **Z553814X**. This can be confirmed online.

Where people have contact with personal data within the IRC ISMS scope, they must be aware of the University of Leeds Code of Practice on Data Protection. The IRC ISMS procedures set out how care must be taken to see that:
1. Personal data are kept securely and screens or monitors are efficiently cleared
2. Personal data are kept away from unauthorised persons
3. Instructions have been received as to whom may be given authorised data access

The DPA distinguishes between ordinary personal data such as address and sensitive personal data. Under the Act the processing of sensitive data requires stricter conditions and explicit consent for collection and processing.

A1.2 Freedom of Information Act 2000

The public has the right to obtain information held by public authorities unless there are good reasons to keep it confidential. As a public body, the University must comply with the Act. The University publishes details of obtaining information under the Act on its website, at www.leeds.ac.uk/freedom-of-information.

A1.3 NHS Act 2006 Section 251

Section 251 of the NHS Act 2006 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes. The Regulations that enable this power are called the Health Service (Control of Patient Information) Regulations 2002. Any references to 'section 251 support or approval' refer to approval given under the authority of the Regulations.

Section 251 enables the common law duty of confidentiality to be overridden to enable disclosure of confidential patient information for medical purposes, where it is not possible to use de-identified information and where seeking consent is not practical, having regard to the cost and technology available.

The Act exists in law for England and Wales and permits the disclosure (by data controllers) and use of identifiable patient information without consent.
Since the Health and Social Care Act 2012 the statutory body with responsibility for Section 251 has been the Confidentiality Advisory Group (CAG) of the Health Research Authority (HRA).