LONDON'S GLOBAL UNIVERSITY

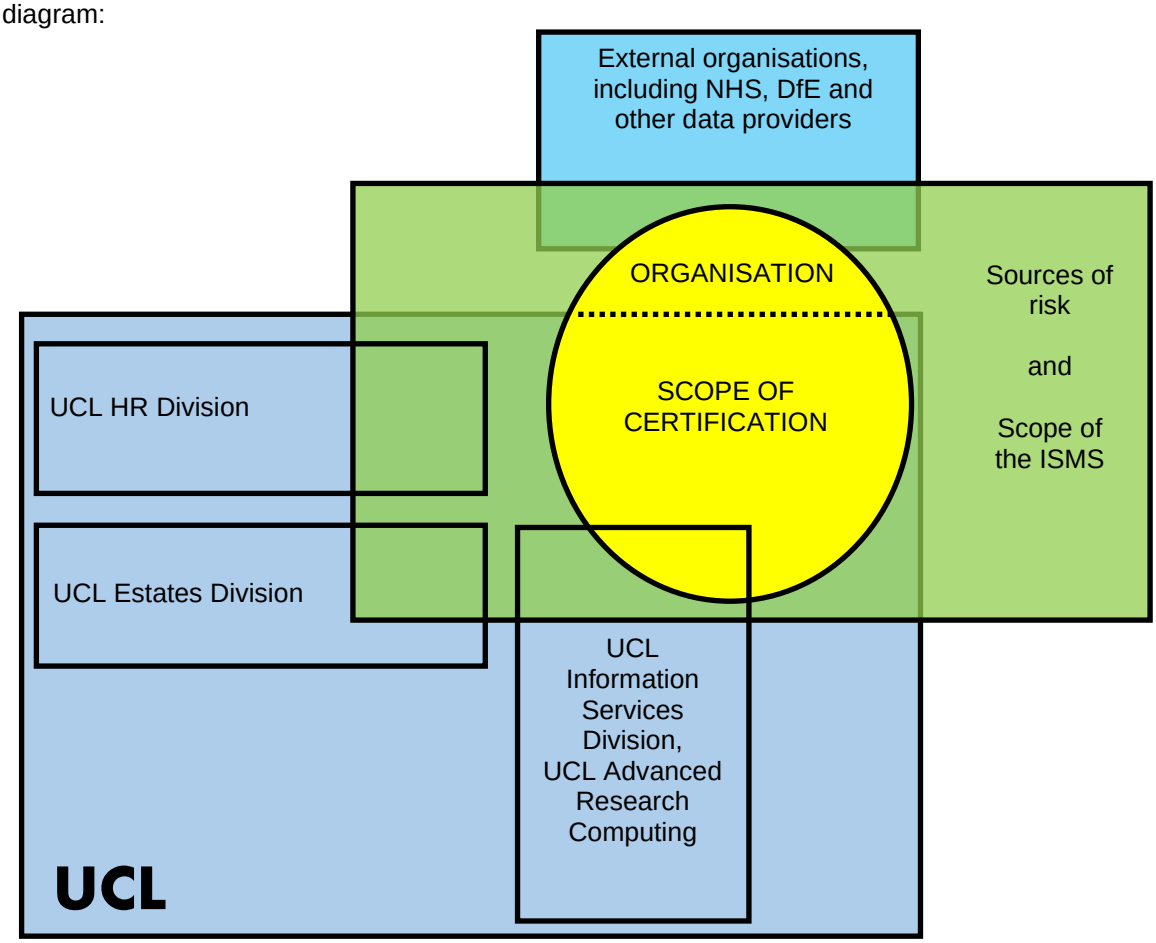
UCL-IG31 Data Safe Haven ISO 27001 Scope

1. Document Information	
Document Name	UCL-IG31 Data Safe Haven Scope of Information Security Management System (ISMS)
Author	Trevor Peacock
Issue Date	31/03/2022
Categorisation	Normal
Next review	One year

2. Document History		
Version	**Date**	**Summary of change**
0.1	24/03/2014	Draft circulated
0.2	06/05/2014	Updates made after feedback from D Brewer
1.0	07/05/2014	Original draft by Alice Garrett approved by T Peacock
1.1	03/09/2014	Updated to incorporate feedback from Stage 2 Audit (C. Furlong)
2.0	23/09/2014	Approved by the chair of IGSG
2.1	09/05/2017	Refresh, consistency check and incorporated observations from audit
2.1	10/05/2017	Interim approval by the chair of IGSG, pending broader discussion at IGSG, June 2017
3.0	27/06/2017	Approved by the chair of IGSG
3.1	05/11/2018	Reviewed by IG Officer and IG Lead
4.0	07/02/2019	Approved by Chair of IG Steering Group
4.1	30/05/2019	Updated to reflect: the move to a single site; including ISG as point of contact for the Police; move from IG to DSP Toolkit
5.0	18/06/2019	Approved by the chair of IGSG
5.1	03/02/2020	Included reference to geographical locations and expanded internal and external stakeholder sections
6.0	06/02/2020	Approved by the chair of IGSG
6.1	10/05/2021	Amended to reflect dual data centres, additional section added to define elements that are out of scope of the ISMS
7.0	09/06/2021	Approved by the chair of IGSG
7.1	14/03/2022	Updated to reflect changes within the DSH support and top management teams
8.0	31/03/2022	Approved by the Chair of IRGC

1. Scope Overview

This document described the scope of the UCL Data Safe Haven organisation, Information Security Management System (ISMS) and ISO/IEC 27001:2013 certification as illustrated in the below diagram:



This document will explain the:

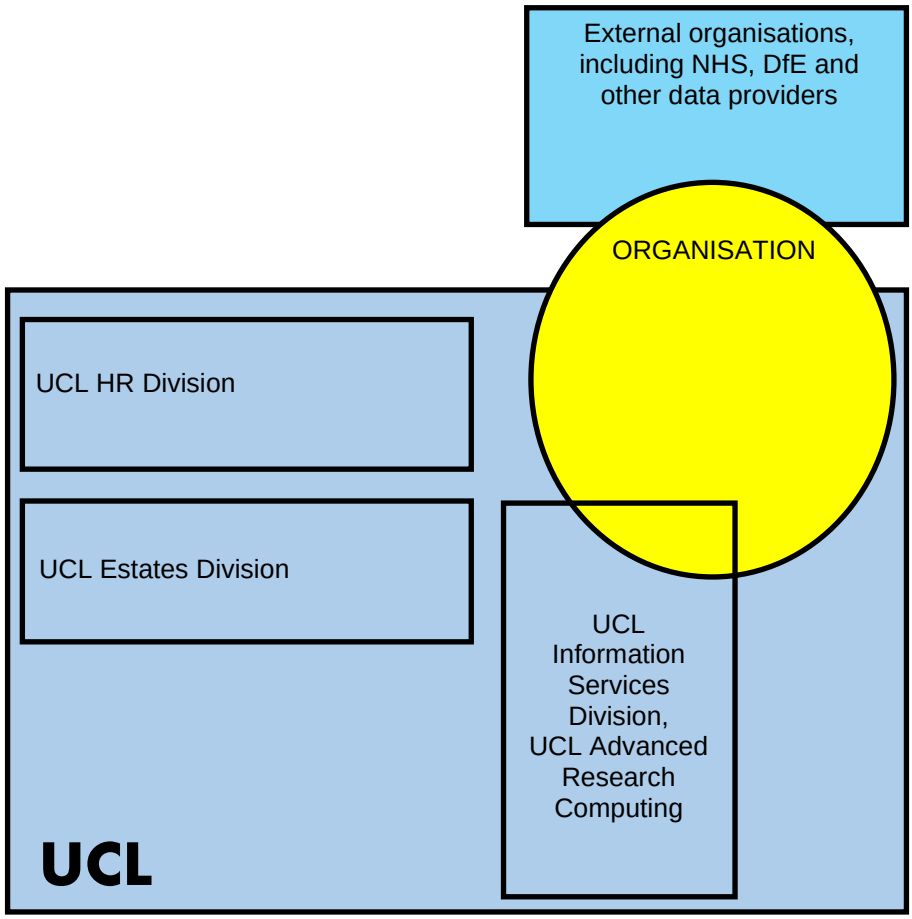
- Scope of the Organisation
- Scope of the ISMS
    - The Technical Environment
    - Sources of Risk and Controls
    - Interested Parties
    - Legal and Regulatory Requirements
- Scope of Certification

2. Scope of the Organisation

The organisation is made up of:

- UCL researchers who use the UCL Data Safe Haven (DSH). These teams are comprised of members of staff, including honorary staff, and students along with external research collaborators. The service was introduced in 2013 and there is a continual flow of new studies adopting the Data Safe Haven.
- Subsets of the following UCL groups, who collectively form the Data Safe Haven Support Team that develops and maintains the technical infrastructure: The Endpoint Management Platforms (EMP) and Cloud Platforms groups, which are part of the Information Services Division (ISD), and the Centre for Advanced Research Computing (ARC).
- Researchers working at UCL are the primary userbase of the Data Safe Haven; the Information Security Group's Information Governance Advisory service provide support, training and advice.

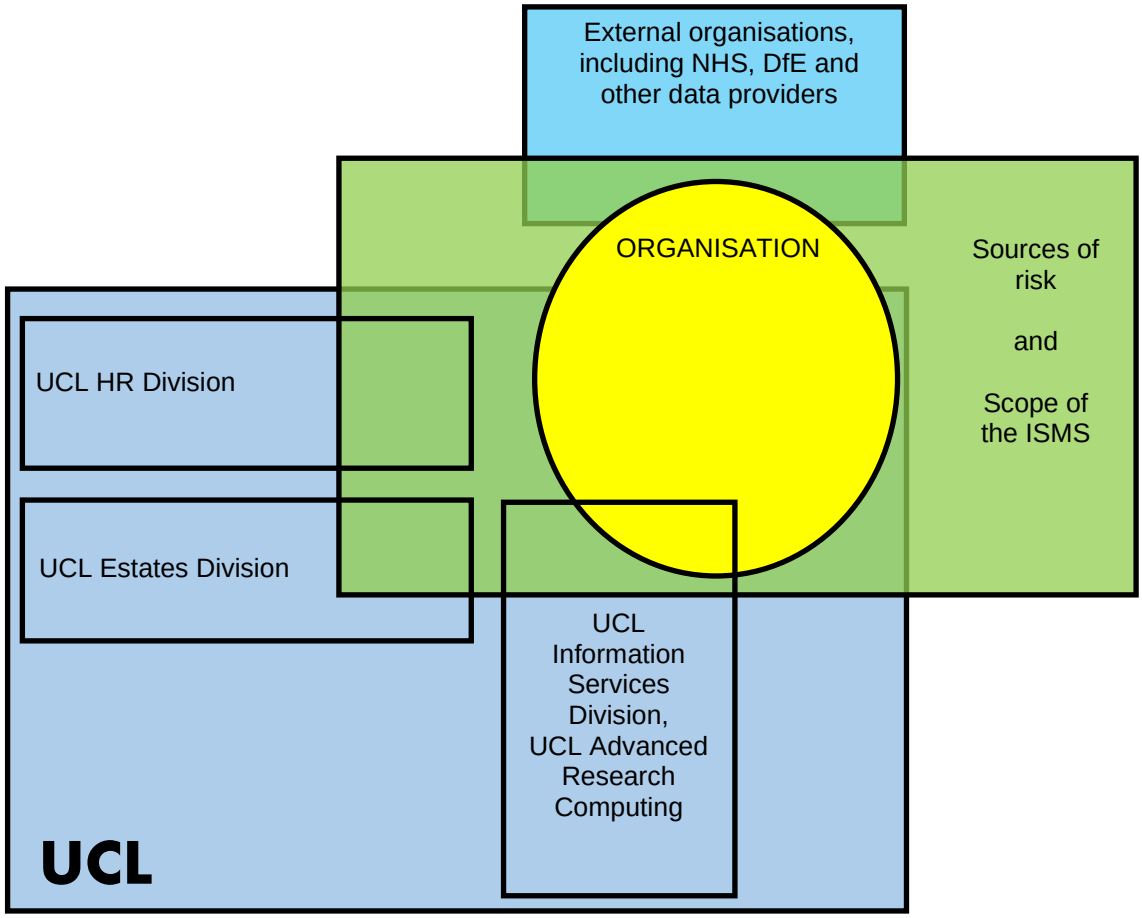
- Members of external organisations (such as NHS Digital, UCL's NHS Partners and the Department for Education) who provide access to confidential information used by UCL researchers within the DSH system.



The purpose of the organisation is to enable researchers to access and use highly confidential information in a secure manner.

The organisation's top management is the Information Risk Governance Committee, chaired by the Senior Information Risk Owner (SIRO).

3. Scope of the Information Security Management System (ISMS)



The Information Security Management System (ISMS) encompasses the organisation itself, the technical environment, sources of risk and controls which may be mandated and carried out by external organisations both inside and outside of UCL. The ISMS is subject to legal, statutory, regulatory and contractual obligations related to information security and security requirements.

3.1 The Technical Environment

The Data Safe Haven (DSH) is a technical environment which has been developed to receive, process and store highly confidential information in a secure manner. The system is designed as a Data Safe Haven with a multi-layered security model incorporating controls to safeguard confidentiality, integrity and availability.

Data is transferred into and out of the DSH using a secure transfer mechanism, available via a web-portal and an encrypted File Transfer Protocol Secure (FTPS) service, including from and to users outside the organisation. An account provisioning process has been established which covers authorisation, registration and 'on-boarding' through to de-registration. Controls have also been put in place to manage the privileged access rights utilised by system administrators. There is a secure log-on procedure for researchers who are required to use dual factor authentication to access the remote desktop environment (a diagram of the system architecture is provided in Appendix A).

Users are prevented from copying data to USB devices and other removable media, the local computer, via drag and drop or cut and paste. Access to web sites from within DSH is subject to risk assessment and is limited to specific sites and only where no other download mechanism is practical. A secure printing service has also been implemented which requires the information asset owner to carry out a risk assessment. Change and capacity management procedures are in place to help maintain system stability. Regular vulnerability scans and annual penetration testing is carried out to verify effectiveness of controls, both by the UCL Information Security Group and by third parties.

The server infrastructure is hosted in secure data centres managed by UCL. The data centres are protected by a set of physical and logical controls.

A full summary of applicable Annex A controls plus those that have been defined by the organisation itself is given in the 'Statement of Applicability'.

3.2 Sources of Risk and Controls

11 primary sources of risk to the organisation have been identified:

1. User deliberately or accidentally leaks information
2. User accidentally or deliberately damages information
3. Premises Break-in
4. Acts of God, Vandals and Terrorists
5. Theft or loss of mobile devices
6. Software failure
7. Hardware Failures
8. Power Failure
9. Internet/Communications Failure
10. Hacking
11. Denial of Service

Whilst some of the sources of risk come from the organisation itself (i.e. user deliberately or accidentally leaking information) some originate from sources outside of the organisation (e.g. hacking).

The controls which form part of the ISMS may be mandated and carried out by the organisation itself; mandated by an external party but carried out by the organisation or mandated and carried out by an external party. This is why the UCL HR Division, UCL Estates Division and parts of the IS Division which are not part of the organisation fall within the scope of the ISMS. They are responsible for carrying out and sometimes mandating controls such as the disciplinary process, maintaining physical entry controls and looking after the UCL network infrastructure. All geographical locations in scope of the ISMS (datacentres and support environments) are subject to a physical risk assessment.

3.3 Interested Parties

Within UCL

The UCL Information Security Group (ISG) is part of ISD and responsible for driving the Information Security agenda within UCL as a whole. The ISG manage UCL-wide information security policies that are mandated across UCL; where these policies and processes are more restrictive, they will take precedence. The Chief Information Security Officer is a member of the IRGC to ensure that their views are represented in management review.

The Data Safe Haven Support Team, as detailed in section 2, Scope.

The Operational Management Group, which formally coordinates and manages the ISMS. This group is formed of members of the Data Safe Haven Support Team.

The organisation's top management is the Information Risk Governance Committee, chaired by the Senior Information Risk Owner (SIRO). The IRGC expects to receive reports on the performance of the ISMS and associated documentation for review and approval.

UCL has four Research and Development offices, linked to its partner NHS trusts: Great Ormond Street; Moorfields; The Royal Free; University College London Hospital. UCL also works with other NHS bodies, such as Central and North West London (CNWL) NHS Trust, Camden & Islington NHS Trust along with others. The R&D offices work with researchers in relation to funding and areas of regulatory compliance, which the DSH is designed to meet.

Researchers within the organisation depend upon the ISMS to meet contractual requirements relating to research data and are required to undertake information governance training, with an annual refresher.

A DSH User Group provides a forum for informing and consulting current and prospective users of the DSH within UCL.

Internal auditors require an audit schedule and expect to have access to documented information and personnel associated with the ISMS.

External to UCL

UCL's partner NHS trusts have many data sharing agreements with UCL researchers, who manage the highly confidential information that they provide. The Head of Clinical Research Governance and Compliance from the UCL / UCLH Joint Research Office is a member of the Information Risk Governance Committee, to ensure that the views and requirements of NHS partners are represented.

NHS Digital manages access to national healthcare datasets. The IG Lead maintains regular contact with NHS Digital to understand changing requirements and to manage compliance with NHS Digital's mandated DSP Toolkit assurance mechanism. The IG Lead is a member of the Information Risk Governance Committee.

Research participants are informed via UCL's privacy notices that their data will be handled subject to technical and organisational safeguards, therefore have an expectation that their data will be protected in this way.

Suppliers of technical equipment, software and services require documented information about requirements that their services must meet.

Suppliers of non-technical resources, such as external audit, require documented information relating to the ISMS.

3.4 Legal and Regulatory Requirements

Legislative and Statutory:

- The Data Protection Act 2018 (DPA18), is enacted by the Information Commissioner's Office. The UCL Data Protection Officer acts as a point of liaison between UCL and the ICO on these matters. The UCL Data Protection Office is responsible for the data protection registration of studies within the organisation and for ensuring compliance with the DPA and Common Law Duty of Confidentiality. The Data Protection Officer is a member of the Information Risk Governance Committee to advise on DPA matters and to report on developments in this area.
- Contact with the Police, within the context of information security, is managed by the UCL Information Security Group (ISG). The Chief Information Security Officer is a member of the Information Risk Governance Committee to advise on matters relating to information risk and security.
- The Confidentiality Advisory Group (CAG), under the Health Research Authority (HRA) oversees applications under the Health Service (Control of Information) Regulations 2001 - Section 251 of the NHS Act 2006. The IG Lead has regular contact with the HRA.
- The Department for Education provides data used by UCL Researchers under the The Education (Individual Pupil Information) (Prescribed Persons) (England) Regulations 2009 and related legal powers.
- Right to work and DBS checks are managed through the UCL HR Employment Contract Administration Office.

Regulatory:

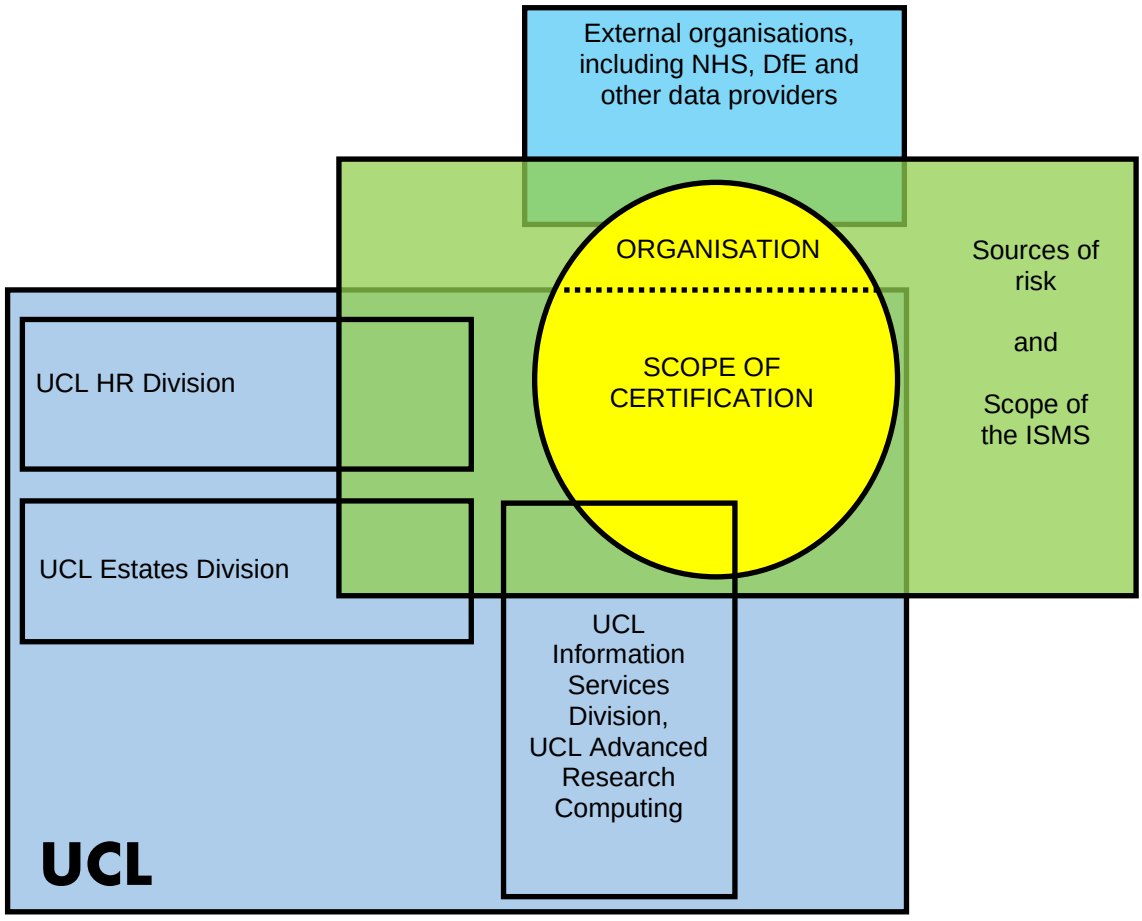
- NHS Digital manages information governance assurance for several data sources, including the Office of National Statistics (ONS) and Hospital Episode Statistics (HES).

- NHS Digital also manages the DSP Toolkit, which is a requirement for applications under Section 251 (see legislative and statutory section above), also for HES and in many cases, for working with data from other sources within the NHS. The DSP Toolkit is revised annually so processes and documentation need to be kept up to date.
- The organisation's Information Security Management System complies with ISO/IEC 27001:2013.
- Medical trials are subject to audit by the Medical and Healthcare products Regulatory Agency (MHRA) which includes audit of information security

UCL Policy:
Users of the Data Safe Haven are subject to UCL policies, including:

- UCL Computing Regulations
- UCL Data Protection Policy
- UCL Information Security Policy

4. Scope of Certification



The scope of the UCL Data Safe Haven ISO/IEC 27001:2013 certification covers the researchers who use the DSH and the ISD, ARC and ISG teams who provide technical support, training and advice. They are all located within UCL managed buildings.

External parties, supplying data, who would fall within the scope of the organisation will not be included in the scope of the certification as they can provide data through the Data Safe Haven environment but are not full users (they have no access to other data or even the data which they have uploaded themselves once the process is complete).

5. Out of scope

The scope defines a clear boundary within which risks are managed. Data transfers outside of the boundary are outside of this scope.

The following are examples of activities outside of the scope of the ISMS:

- Data, once exported from the Data Safe Haven, including printing
  - *Controls protect data up to the point of delivery*

- Endpoint devices used to connect to the Data Safe Haven
  - *Controls prevent data from being copied from within the thin client environment to endpoint devices*