Research Information Governance Policy

1. Document Information	
Document Name	SLMS-IG03 Research Information Governance Policy
Author	Alice Garrett
Issue Date	04/06/2018
Approved By	Chair of SLMS IGSG
Next review	04/06/2021

2. **Document History**

Version	Date	Summary of change
0.1	14/12/2012	First draft for discussion
0.2	17/12/2012	Incorporated feedback from Trevor Peacock
0.3	03/01/2013	Incorporated feedback from Patrick Malcolm
0.4	04/01/2013	Incorporated feedback from Anthony Peacock
0.5	31/01/2013	Incorporated feedback from T. Peacock, A. Garrett and S. Murphy
0.6	14/03/2013	Incorporated feedback from B.Kenyon, A. Peacock, A.Garrett and S.Murphy
1.0	02/08/2013	Approved by Chair of the SLMS IGSG
1.1	15/04/2014	T. Peacock – addition of sections and wording to improve alignment with ISO27001:2013
2.0	06/05/2014	Approved by Chair of the SLMS IGSG
2.1	12/06/2014	T.Peacock - Included item 6.9, reference to SLMS-IG15
3.0	23/09/2014	Approved by Chair of the SLMS IGSG
3.1	27/11/2014	T Peacock – incorporated comments from internal audit and Michael Abtar
3.2	05/12/2015	Incorporated feedback from Bridget Kenyon and Kim Kingan
4.0	11/12/2014	Approved by Chair of the SLMS IGSG
4.1	01/03/2015	Inclusion of timescales for metrics and section on access control T. Peacock
5.0	20/03/2015	Approved by Chair of the SLMS IGSG
5.1	20/05/2018	Reviewed by Jack Hindley
6.0	04/06/2018	Approved by Chair of IG Steering Group
6.1	31/01/2020	Change SLMS references to UCL, update metrics, include terminology reference

7.0	06/02/2020	Approved by Chair of IG Steering Group

3.0 Introduction

3.1 Information is a vital asset, both in terms of the world leading clinical research undertaken by University College and in terms of the efficient management of services and resources.

3.2 It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures, management accountability and structures are in place to provide a robust governance framework for information management, which is covered, in general, by UCL's Data Protection and Information Security policies.

3.3 Research projects frequently receive information from third parties including the NHS which is restricted by specific regulation or contracts. As a result, UCL is subject to additional responsibilities in satisfying information governance requirements and in safeguarding highly confidential information. As such, it is the responsibility of all members of UCL to ensure that information is managed appropriately.

4.0 Scope of this Policy

4.1 For the purposes of this and related policies, that form the Information Governance Framework outlined below, information is defined as data that can be stored in any format, including:

4.1.1 Structured record systems: paper and electronic;

4.1.2 Unstructured information: paper and electronic;

4.1.3 Transmission of information by any media.

4.2 This policy covers any research data that could potentially identify individuals or is restricted by regulation or contract, within UCL, including information relating to past, present and potential research subjects.

4.3 This policy covers all information systems purchased, developed and managed by, or on behalf of UCL.

4.4 This policy is in addition to the UCL Data Protection Policy and UCL Information Security Policy and applies to all staff, honoraries and students of UCL and all other computer, network or Data Users authorised by UCL or any department thereof. It relates to their use of any UCL-owned facilities (and those leased by or rented or on loan to UCL), centrally managed or otherwise; to their use of all private systems (whether owned, leased, rented or on loan) when connected to the UCL network; to their use of all UCL-owned or licensed information and programs (wherever stored); and to their use of all information and programs provided to UCL by sponsors or external agencies (wherever stored).

4.5 For the avoidance of doubt where this policy is at variance with another UCL policy the more restrictive policy will apply.

5.0 Scope of Information Governance

5.1 Information Governance is a framework to enable UCL to handle information including highly confidential information, legally, securely, efficiently and effectively. It is formed of the following initiatives and related policy documents:

Initiative	Policy document
Information Governance Management	SLMS-IG03 Research Information Governance Policy
Information Security Assurance	UCL Information Security Policy
Confidentiality & Data Protection Assurance	UCL Data Protection Policy
Information classification and labelling	UCL Information Management Policy

6.0 Principles

6.1 UCL recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

6.2 UCL fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, personal information about research subjects.

6.3 UCL also recognises that, where it is necessary to share personal and highly confidential information with other organisations and agencies, this needs to be carried out lawfully, and in a manner consistent with the interests of data subjects and, in some circumstances, the public interest.

6.4 UCL believes that accurate, timely and relevant information is essential to world leading research and the university's strategic academic goals. As such, it is the responsibility of all members of UCL to ensure that information is managed appropriately. UCL will work with information providers to ensure that research subjects are aware of the need for UCL to hold their personal information, the processes that UCL uses, and the rights they hold as data subjects.

6.5 UCL undertakes to maintain high standards of information handling by reference to the HORUS model, where information is:

- Held securely and confidentiality;
- Obtained fairly and efficiently;
- Recorded accurately and reliably;
- Used effectively and ethically;
- Shared appropriately and lawfully.

6.6 UCL seeks to protect its computer systems from misuse and to minimise the impact of service breaks through conformance with the ISO/IEC 27001:2013

information security standard and the continual development of an Information Security Management System (ISMS).

6.7 UCL will ensure that personal data and other confidential information within its control are held, retained, and disposed of in line with legislation, regulation and contracts.

6.8 UCL will obtain and share information in compliance with the common law duty of confidentiality.

7.0 Information Security Objectives and Continual Improvement

7.1 The objective of this organisation is to enable research to be carried out on confidential information in a suitably secure manner. This is measurable by:

Objective	Metric	Target
Appropriate management of risk	The proportion of applicable studies / teams using the Data Safe Haven	100%
	The level of risk within the organisation as assessed by our partners	No degradation of risk
	The level of risk within the organisation as measured in the UCL Data Safe Haven Risk Assessment	All risks are 'green'
Manage risk of: Data User deliberately or accidentally leaks information User accidentally or deliberately damages information	The proportions of Data Safe Haven Data Users, Information Asset Owners and Information Asset Administrators completing approved training annually.	95% completion rate for each group

7.2 The above metrics, together with audit observations will be monitored to ensure a continual improvement in information security

7.3 More detailed information security objectives shall be detailed in the IG Improvement plan. The plan shall be reviewed annually or as the result of significant organisational or legislative change and updated to include:

i. additional requirements relating to the latest version of the NHS Data Security and Protection Toolkit

ii. improvements identified through risk assessment and risk treatment

7.4 In response to the above assessment, UCL will formulate an Information Governance Improvement Plan each year, which will detail the action plans that

have been raised through the Data Security and Protection Toolkit and ISMS, along with the expected risks and benefits.

7.5 An annual ISO/IEC 27001 surveillance audit shall be carried out to ensure that the Information Security Management System (ISMS) is suitable, adequate and effective for the needs of the organisation.

8.0 Legal and Regulatory Requirements

8.1 Legislative and statutory:

The EU General Data Protection Regulation (2016) and the UK Data Protection Act (2018), are enforced 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 this legislation and the Common Law Duty of Confidentiality. The Data Protection Officer will be a member of the IGSG to advise on legislative matters and to report on developments in this area

8.2 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 will have regular contact with the HRA.

8.3 Regulatory:

NHS Digital manages information governance assurance for a number of data sources, including the Office of National Statistics (ONS), Hospital Episode Statistics (HES)

8.4 NHS Digital also manages the Department of Health's Data Security and Protection Toolkit, a requirement for applications under Section 251 (see legislative and statutory section above) and also for HES and, in many cases, for working with data from other sources within the NHS.

8.5 The organisation's Information Security Management System, the scope of which is defined in the SLMS-IG31 Data Safe Haven Scope, will be certified to the ISO/IEC 27001:2013 information security standard

8.6 Medical trials are subject to audit by the Medical and Healthcare products Regulatory Agency (MHRA) which includes audit of information security

9.0 Management & Accountability

9.1 Information Governance management across UCL will be coordinated by the Information Governance Steering Group, the Terms of Reference for which are defined in 'SLMS-IG01 IG Steering Group Terms of Reference'.

9.2 The Information Governance Steering Group will be accountable to the UCL Senior Management Team.

9.3 The Information Governance Lead and Senior Information Risk Owner (SIRO) will be an Executive Director with responsibility for Information Governance within UCL

9.4 Roles and responsibilities will be detailed in SLMS-IG32 IG Framework Roles and Responsibilities

9.5 Additional guidance is given in SLMS-IG04a Data Handling Guidance. Where there is a deliberate, or totally negligent breach of this policy, the matter will be dealt with under the UCL Disciplinary Policy and Procedure. UCL wishes to encourage a transparent and open "lessons learnt" culture. Consequently, UCL

will deal sympathetically with all breaches, providing guidance and training to those impacted by the breach when such breaches are found to be accidental.

9.6 Information security is the responsibility of all individuals directly employed or otherwise by UCL; all information incidents must be reported promptly and openly in accordance with SLMS-IG15 Incident Reporting Procedure

10.0 Awareness & Training

10.1 Information Governance training shall be included as standard for staff inductions.

10.2 All staff and researchers within scope of this policy shall complete the IGSG's approved Information Governance Training as per the SLMS-IG16 Training Needs Analysis.

10.3 Supplementary or role-based training shall be given, or organised, where necessary; this can be requested by an individual wanting personal development or arranged at the discretion of a manager.

10.4 UCL shall also ensure that awareness of Information Governance and related matters is maintained and measured, and that new advice or initiatives are communicated through a wide range of different channels.

11.0 Risk

11.1 In consultation with the SIRO, Information Asset Owners will ensure that the project/team improvement plan accurately reflects any data protection and privacy risks arising from their projects/team and that suitable remediation plans are in place to manage/eliminate these risks. For more detail see SLMS-IG06 IG Improvement Plan.

12.0 Review and monitoring of compliance

12.1 This policy will be reviewed every three years (or sooner if new legislation, codes of practice or national/international standards are introduced or revised).

12.2 The implementation and compliance with this Policy will be monitored by the IGSG.

12.3 UCL will seek to undertake or commission a range of audits when and where necessary and reports will be presented to the IGSG to monitor compliance. Action plans will be devised to deal with any identified issues.

12.4 Compliance with this policy will be monitored during the investigation of complaints or incidents and identified risks.

13.0 Access Control

13.1 Within the ISMS, Data Users will act in accordance with the SLMS-IG36 Data Safe Haven Access Control Policy

13.2 UCL will ensure that confidentiality of information is maintained and access granted appropriately and only to authorised personnel. There must be a clear

separation of access rights where different members of a single team are working on separate data sets.

13.3 Data Users shall only be provided with access to the network and network services that they have been specifically authorised to use.

13.4 A formal registration and de-registration process shall be implemented to enable assignment of access rights.

13.5 A formal access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

13.6 Access to systems and applications shall be controlled by a secure log-on procedure. The allocation of secret authentication information shall be controlled through a formal management process.

13.7 The allocation and use of privileged access rights shall be restricted and controlled. Password management systems shall be interactive and shall ensure quality passwords.

13.8 Information Asset Owners shall review Data Users' access rights at regular intervals.

13.9 The access rights of all Data Users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

14.0 Conventions used in this document

14.1 UCL policies currently employ different terminology to the DSP Toolkit. The following terms are equivalent:

DSP Toolkit and this policy	**UCL policies**
Information Asset Owner	Data Owner
Information Asset Administrator	Data Custodian

The above are included in the more general class of **Data User**, used within UCL policies.

UCL's glossary of terms:

https://www.ucl.ac.uk/information-security/sites/information-security/files/glossary.pdf