CLS Research Information Governance Policy

1. Document Information	
Document Name	CLS-IG03 Research Information Governance Policy
Author	Gearoid Garvey
Issue Date	26/03/2015
Approved By	Chair of CLS IGSG
Next review	01/12/2015

2. Document History		
Version	**Date**	**Summary of change**
0.1	26/03/2015	First draft for discussion
0.2	27/03/2015	Incorporated feedback from CLS IGSG
1.0	27/03/2105	Approved

This document includes data that is **PUBLIC** and can be disclosed outside UCL IOE CLS and used, or disclosed in whole or in part for any purpose other than to evaluate and implement procedures defined within this document.

1.0 Introduction

1.1 Information is a vital asset, both in terms of the world leading clinical research undertaken by UCL's Institute of Education's School – the Centre for Longitudinal Studies (CLS) and in terms of the efficient management of services and resources.

1.2 Research projects within the CLS frequently receive information from third parties including the NHS, DfE, etc. As a result, CLS is subject to additional responsibilities in satisfying information governance requirements and in safeguarding sensitive information.

1.3 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.

1.4 Accurate, timely and relevant information is essential to meeting the strategic academic goals of CLS; the general principles of which are covered in the UCL Data Protection and CLS Information Security Policies. As such, it is the responsibility of all members of CLS to ensure that information is managed appropriately.

2.0 Scope of this Policy

1.1 For the purposes of this and related policies, that form the Information Governance Framework outlined in 3.1 below, information is defined as data that can be stored in any format, including:

- Structured record systems: paper and electronic;
- Unstructured information: paper and electronic;
- Transmission of information: fax, email, post, telephone, including text messages.

2.1 This policy covers all aspects of handling personal data[1], sensitive personal data[2] and other pseudonymised research data that could potentially identify individuals, within CLS, including information relating to past, present and potential research subjects.

2.2 This policy covers all information systems purchased, developed and managed by, or on behalf of, CLS and any individual directly employed or otherwise by CLS.

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

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

[1] For definition please see Data Protection Act 1998 Section 1
[2] For definition please see Data Protection Act 1998 Section 2

3.0 Scope of Information Governance

3.1 Information Governance is a framework to enable CLS to handle information including sensitive personal data, legally, securely, efficiently and effectively. It is formed of the following initiatives and related policy documents:

Initiative	Policy document
Information Governance Management	CLS-IG03 Research Information Governance Policy (this document)
Information Security Assurance	CLS Information Security Policy
Confidentiality & Data Protection Assurance	UCL Data Protection Policy

4.0 Principles

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

4.2 CLS 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.

4.3 CLS also recognises the need to share personal and sensitive personal data with other organisations and agencies in a controlled manner consistent with the interests of the subject and, in some circumstances, the public interest.

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

4.5 CLS 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.

4.6 CLS seeks to protect its computer systems from misuse and to minimise the impact of service breaks through conformance with best practice e.g. the standard ISO/IEC 27001:2013 and the continual development of an Information Security Management System (ISMS).

4.7 CLS will ensure that the personal and sensitive personal data within its control are held, retained, and disposed of in line with good practice and the law.

4.8 CLS will obtain and share information in compliance with the common law duty of confidentiality.

5.0 Information Security Objectives and Continual Improvement

5.1 The objective of this organisation is to enable research to be carried out on identifiable data in a suitably secure manner. This is measurable by:

Objective	Metric	Target
Appropriate management of risk	Regular monitoring of the CLS Risk Register at monthly Principal Investigator (PI) meetings.	Reviews of IG related risks to feed into planned quarterly IGSG meetings.
	Level of risk within our contracted suppliers as assessed via regular and annual independent audits.	No degradation of risk
	The level of risk within the organisation as measured in the CLS Risk Register	All relevant risks are 'green'
Compliance with the requirements of external parties e.g. HSCIC	The successful completion annually of an NHS IG Toolkit submission.	100%
Manage risk of: User deliberately or accidentally leaks information User accidentally or deliberately damages information	The number of staff receiving training and awareness and the effectiveness of it	All CLS staff to complete IG training as part of their induction and annual refresh training thereafter – as per CLS IG Training Strategy.

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

5.3 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 IG Toolkit

ii. improvements identified through risk assessment and risk treatment

5.4 In response to the above assessment, CLS will formulate an Information Governance Improvement Plan each year, which will detail the action plans that have been raised through the IG Toolkit, along with risks and benefits.

6.0 Legal and Regulatory Requirements

6.1 Legislative and statutory:

The Data Protection Act 1998 (DPA), 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 will be invited to IGSG to advise on DPA matters and to report on developments in this area

6.2 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.

6.3 Recital 26 and Article 27 of the European Data Protection Directive (95/46/EC) in relation to anonymisation and pseudonymisation

6.4 Regulatory:

The HSCIC manages information governance assurance for a number of data sources, including the Office of National Statistics (ONS), Hospital Episode Statistics (HES). The IG Lead maintains contact with HSCIC via the NHS-HEI IG working Group and during applications to the HSCIC for access to data for either research or tracing.

6.5 The HSCIC also manages the Department of Health's IG Toolkit, of which the Hosted Secondary Use Team / Project (HSUTP) 'view' is 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. The IG Toolkit is revised annually so processes and documentation needs to be kept up to date.

7.0 Management & Accountability

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

7.2 The CLS Information Governance Steering Group will be accountable to the CLS Senior Leadership Team and report centrally via the emerging UCL Information Risk Governance framework.

7.3 The Senior Information Risk Owner (SIRO) will be a Director with responsibility for Information Governance within CLS. The IG Lead role is currently held by the Senior Operations Manager in CLS.

7.4 Roles & responsibilities are detailed in CLS IG Framework Roles and Responsibilities

7.5 Additional guidance is given in CLS's Confidentiality Code of Conduct'. Where there is a deliberate or totally negligent breach of this policy, the matter will be dealt with under the appropriate organisational 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.

7.6 Information security is everyone's responsibility; all information incidents must be reported promptly and openly in accordance with CLS's Information Reporting Procedure

8.0 Awareness & Training

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

8.2 All staff shall complete the CLS's IGSG's approved IG Training.

8.3 All external users of data who wish to access data within CLS premises, as part of their contracted role, must complete CLS's IGSG's approved IG Training for that role.

8.4 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.

8.5 **CLS 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.

9.0 Risk

9.1 In consultation with the SIRO, the Senior Leadership Team will ensure that the cohort study/team improvement plan accurately reflects any data protection and privacy risks run by their projects/team and that suitable remediation plans are in place to manage/eliminate these risks. For more detail see the Improvement Plan.

10.0 REVIEW AND MONITORING COMPLIANCE

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

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

10.3 UCL-IOE will seek to undertake or commission a range of internal and external 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.

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