UK Longitudinal Linkage Collaboration
Population Health Sciences
Bristol Medical School
Canynge Hall
39 Whatley Road
Bristol BS8 2PS

UK Longitudinal Linkage Collaboration (UK LLC)

INFORMATION SECURITY POLICY

PUBLIC

Version 1.7

13 February 2024

Policy number:	POL-ISM-001	**Version:**	V1.7
Author:	Katharine Evans, Governance & Policy Manager	**Date:**	24/01/2022
Authorised by:	Andy Boyd, Director	**Date:**	08/02/2022
Date published:	08/02/2022	**Date to review:**	09/02/2025
Permission to edit this policy must be provided by:	Director; Head of Operations; Senior Data Manager (Governance & Users)		

Review History

Version:	Review Date:	Reviewed by:	Section(s) amended:	Authorised by:
1.1	30/05/2022	Katharine Evans, Governance & Policy Manager	Section 1 – minor updates to text & added new principle re risk	Andy Boyd, Director
1.2	12/09/2022	Katharine Evans, Governance & Policy Manager	Section 1 – added information to give broader context for a public facing policy	Andy Boyd, Director
1.3	20/10/2022	Katharine Evans, Governance & Policy Manager	Review of whole policy to ensure alignment with DEA requirements	Andy Boyd, Director
1.4	15/12/2022	Katharine Evans, Governance & Policy Manager	Section 6 – updated with link to all UK LLC Policies & SOPs	Andy Boyd, Director
1.5	11/05/2023	Katharine Evans, Governance & Policy Manager	Section 1 – added DEA accreditation; Section 5 – updated objectives	Andy Boyd, Director
1.6	31/10/2023	Hannah Woodward, Information Security Officer	Updated logos & section 5.4 – added BCP, Info Sec Policy & restricted System Dev Policy to data team in mandatory documents	Andy Boyd, Director
1.7	13/02/2024	Katharine Evans, Senior Data Manager (Gov & Users)	Updated IS objectives	Andy Boyd, Director

Contents – UK LLC Information Security Policy

1. INTRODUCTION

1.1 Background

The UK Longitudinal Linkage Collaboration (UK LLC) organisation is led by the University of Bristol (UoB) and operated in collaboration with the University of Edinburgh (UoE). UK LLC manages the collation, curation and access to data about Longitudinal Population Study (LPS) participants held in the UK LLC Trusted Research Environment (TRE).

All data held about LPS participants are de-identified, which means that no one at UK LLC or any of the researchers who access data in the TRE can see participants' personal identifiers, such as name or address.

Identities are protected by a de-identification process conducted by an NHS Trusted Third Party (NHS Digital Health and Care Wales) and technical, physical and procedural safeguards at Secure eResearch Platform UK (SeRP UK, Swansea University), the infrastructure that hosts the UK LLC TRE. Furthermore, all analytical outputs from the UK LLC TRE are checked by experts to make sure individuals can not be identified.

Safeguarding the anonymity and security of participants' data stored in the TRE are of paramount importance to UK LLC.

This policy will be reviewed to respond to any changes in the UK LLC risk assessment or risk treatment plan and at least annually.

1.2 Purpose

This policy sets out UK LLC's approach to safeguarding the anonymity of individual participants, ensuring the security (confidentiality, integrity and availability) of the data stored in the UK LLC TRE and safeguarding legislative compliance.

Confidentiality	Access to information shall be restricted to those with appropriate authority and a business need to access the information.
Integrity	Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
Availability	Information shall be available and delivered to the right person at the time when it is needed.

This policy should be read in conjunction with the UK LLC Data Access and Acceptable Use Policy, which explains why UK LLC was established and details UK LLC's commitments to LPS participants, data owners and researchers, and the rules, processes and procedures that approved researchers agree to follow when accessing the TRE.

1.3 UK LLC's Information Security Management System (ISMS)

The UK LLC organisation manages the collation, curation and access to data held in the UK LLC TRE. To provide assurance to the public, LPS participants, the contributing LPS, the NHS and other national data providers, UK LLC wishes to demonstrate industry best practice information security through the development, maintenance and continual improvement of an information security management system (ISMS).

An ISMS is a framework of policies and procedures that include all legal, physical and technical controls that an organisation has put in place to safeguard its information assets.

UK LLC is ISO 27001 certified, completes the annual NHS Data Security and Protection Toolkit (DSPT) and has been accredited by the UK Statistics Authority as a processing environment under the Digital Economy Act (DEA).

1.3.1 ISO 27001

ISO 27001 is an internationally recognised best practice standard for an ISMS. UK LLC's ISMS was ISO 27001 certified by independent industry assessors in August 2022 (Certificate Number 21069).

1.3.2 NHS DSPT

NHS DSPT enables organisations to measure their performance against the National Data Guardian's 10 data security standards. UK LLC completes the annual DSPT audit (Organisation Code EE133799-LLC).

1.3.3 UK Statistics Authority

UK LLC was accredited by the UK Statistics Authority in March 2023 for the preparation and provision of data under the DEA – see List of Digital Economy Act Accredited Processing Environments – UK Statistics Authority

2. SCOPE

The UK LLC ISMS spans two organisations: the **University of Bristol** (UoB) and the **University of Edinburgh** (UoE). This policy therefore collates and refers to guidance from both parent organisations, and then, where necessary, applies specific UK LLC requirements, to provide a standard approach within UK LLC.

All UK LLC staff must adhere to this Information Security Policy.

This policy and the associated ISMS apply to all UK LLC information and physical assets, processes, procedures and staff; UoB suppliers of critical functions to UK LLC; and third party data processors within the scope of the deployed ISMS (UoB and UoE).

This means that all UK LLC staff will be made aware of their responsibilities to preserve information security, to report information security weaknesses, events and incidents, and to act in accordance with the requirements of the ISMS.

All UK LLC staff will receive information security awareness training and more specialised UK LLC staff will receive appropriately specialised information security training.

The consequences of breaching this policy are set out by the respective parent organisations:

- University of Bristol (UoB) Ordinance 28 Conduct Procedure for Members of Staff: Conduct Procedure - managers' guidance | Human Resources | University of Bristol
- University of Edinburgh (UoE) Disciplinary policy: Disciplinary_Policy.pdf (ed.ac.uk)

3. ABBREVIATIONS

ADR UK	Administrative Data Research UK
CIA	Confidentiality, Integrity, Availability
DEA	Digital Economy Act
DPIA	Data Protection Impact Assessment
DSPT	Data Security and Protection Toolkit
HDR UK	Health Data Research UK
ISMS	Information Security Management System
LPS	Longitudinal Population Study
OMG	Operational Management Group
SOP	Standard Operating Procedure
TRE	Trusted Research Environment
UK LLC	UK Longitudinal Linkage Collaboration
UoB	University of Bristol
UoE	University of Edinburgh

4. ROLES AND RESPONSIBILITIES

Information security is embedded throughout UK LLC and all UK LLC staff have responsibilities towards it. The terms of reference for the Senior Information Risk Owner (SIRO), Information Asset Owners (IAOs) and the Caldicott Guardian are available to all staff (see section 6). All staff should know:

- What information they are using and how it should be handled, stored and transferred
- Their responsibility to raise any information security concerns
- How to report a suspected breach of information security or non-compliance within UK LLC.

Managers should ensure all information security procedures are carried out correctly.

5. INFORMATION SECURITY AT UK LLC

5.1 Key principles

- UK LLC has adopted the 'Plan, Do, Check, Act' approach to operational management
- Risks are identified and managed in the Risk Register. Data Protection Impact Assessments (DPIAs) are developed and maintained for data flows
- The control and processing of data is restricted to UoB UK LLC staff and their contracted data processors

- The management and implementation of the UK LLC application process, communications and public/participant involvement is conducted by UoE and UoB UK LLC staff
- The data UK LLC hold under licence (from LPS and other data owners) shall only be processed and stored within the UK LLC TRE
- The data within the UK LLC TRE shall be ‘functionally anonymous’
- UK LLC is a paper-free organisation
- Removable storage media, e.g. USB flash drives, are not permitted
- Data that flow into the UK LLC TRE are encrypted in transit; physical media transit is not permitted
- UK LLC management ensure all staff are aware of their responsibilities
- UK LLC shall be transparent in its operations.

UK LLC staff must refer to and abide by their respective parent organisation’s guidance (see Tables 1 and 2). Please let the UK LLC Information Security team know if you identify any conflicts between your organisational policy and any UK LLC policy (ukllc-isms@bristol.ac.uk).

5.2 Objectives

Detailed below are the **objectives of the UK LLC Information Security Policy**.

Evidence for each objective is collated and reported to the UK LLC OMG for monitoring. Dates for objectives to be achieved and by which organisation (UoB and UoE) are detailed below each objective in italics.

OBJECTIVES of the UK LLC Information Security Policy:

1. To ensure all UK LLC staff are fully aware of information security and their responsibilities towards it in the UK LLC environment:
   - i. 100%* of staff will have passed annual information security training
     (*excluding staff on long-term absence, e.g. maternity leave)
   - ii. 80% performance measures (external and internal audits, and spot audits of critical business areas) judged to be compliant
   - iii. Staff continue to raise information security queries with IS Team
   - iv. Rising performance indicators
   - v. Increasing trend and confidence to report weaknesses, events and incidents.

Evidence collated by Information Security Officer and Senior Data Manager (Governance & Users).
Targets to be achieved by December 2024.
Applies to UoB and UoE.

2. To ensure all UK LLC data are stored and handled appropriately, maintaining their CIA:
   - i. 90% of internal audits take place on time measuring authorised users and other agreed controls
   - ii. De-identification audit undertaken using the UK Anonymisation Network’s (UKAN’s) Anonymisation Decision-making Framework (ADF) on an at least annual basis
   - iii. Amber information security risks monitored regularly by the OMG.

Evidence collated by Information Security Officer and Senior Data Manager (Governance & Users).
Targets to be achieved by December 2024.
(ii) applies to UoB only; (i) and (iii) apply to both UoB and UoE.

3. To enable UK LLC to meet the general principles of ISO 27001, DEA and NHS DSPT:
   - i. Annual ISMS management review undertaken

ii. Successful audit by an ISO 27001 accredited organisation each year
iii. Successful audit by a DEA accredited organisation each year
iv. Successful audit for NHS DSPT each year
v. Successful maintenance of REC and CAG approvals each year
vi. Improvements monitored regularly via the Continuous Improvement Log.

Evidence collated by Information Security Officer and Senior Data Manager (Governance & Users).
Targets to be achieved by December 2024.
(ii), (iii), (iv) and (v) apply to UoB only; (i) and (vi) apply to both UoB and UoE.

4. To ensure all UK LLC staff are aware of relevant legislation and its implications:

i. Regular update of information security issues (e.g. legislative change) via UK LLC team meeting and emails from ukllc-isms@bristol.ac.uk
ii. Circulating Medical Research Council regulatory support centre guidance within one month of printing.

Evidence collated by Information Security Officer and Senior Data Manager (Governance & Users).
Targets to be achieved by December 2024.
Applies to UoB and UoE.

5. To develop and maintain effective relationships with Swansea University, Digital Health and Care Wales, and Office for National Statistics regarding maintaining and evolving policy and practice:

i. To establish and maintain working contact and networking with IS staff in these organisations to share best practice and to maintain awareness of change (subscription to forum or newsletter)
ii. To consult and work with funders and coordinating networks (HDR UK and ADR UK) regarding sharing of best practice in research IS and governance.

Evidence collated by Director, Co-Director and Head of Operations.
Targets to be achieved by December 2024.
Applies to UoB and UoE.

6. To ensure all staff have successfully completed security clearances:

i. All staff have successfully completed Baseline Personnel Security Standard (BPSS), which includes Disclosure and Barring Service (DBS) security checks. Employment of new staff will be conditional on security clearance.

Evidence collated by Information Security Officer and Senior Data Manager (Governance & Users).
Targets to be achieved by December 2024.
Applies to UoB and UoE.

7. To develop a quarterly reporting system that aligns with UK Statistics Authority's and other organisations' requirements:

i. Key teams including the Data, Applications and IS teams complete quarterly performance reports that align with the requirements stated by the UKSA (and other organisations, as required)
ii. Teams report requested KPIs to the UKSA within two weeks to the standard expected.

Evidence collated by Information Security Officer and Senior Data Manager (Governance & Users).
Targets to be achieved by December 2024.
Applies to UoB and UoE.

5.3 Parent organisation policies

Table 1 Relevant UoB policies that must be read, understood and followed by UoB based UK LLC staff

UoB Policy Name	Summary/Highlights
Information Security Policy: ISP-01v1.2.pdf (bristol.ac.uk)	UoB's paramount policy on information access and security: it defines the responsibilities of individuals with respect to information use and to the provision and use of information processing systems.
Acceptable Use Policy: ISP-09.pdf (bristol.ac.uk)	'Members must ensure that their computers and other devices are locked before being left unattended'.
Mobile and Remote Working Policy: ISP-14.pdf (bristol.ac.uk)	Sets out the additional principles, expectations and requirements relating to mobile and remote/home working.
Information Handling Policy: ISP-07.pdf (bristol.ac.uk)	'Computer screens on which information classified as confidential or above is processed or viewed must be sited in such a way that they cannot be viewed by unauthorised persons.'
Outsourcing and Third Party Compliance: ISP-04-v1.4.pdf (bristol.ac.uk)	Outlines the conditions that are required to maintain the security of UoB's data and systems when contracting external suppliers.
Compliance Policy: ISP-03 v1.2.pdf (bristol.ac.uk)	Outlines UoB's requirement to comply with certain legal and regulatory frameworks – to be read in conjunction with the Guide to Legislation relevant to Information Security Policy: guide.pdf (bristol.ac.uk)

Table 2 Relevant UoE policies that must be read, understood and followed by UoE based UK LLC staff

UoE Policy Name	Summary/Highlights
Information Security Policy: Information security policy (ed.ac.uk)	Details how everyone is responsible for protecting UoE information. It states how UoE ensures that CIA is maintained. Appendix 1 lists all the associated standards, e.g. S.6. Asset Management.
Mobile Device Standard: Minimum, and required reading | The University of Edinburgh (only accessible to UoE staff)	Specifies UoE's minimum mandatory requirements for the use of UoE issued mobile devices and removable media devices.
Information Security Classification Standard: Minimum, and required reading | The University of Edinburgh (only accessible to UoE staff)	Outlines the classification levels data may take within UoE and what controls should be considered as part of protecting and handling data at each level.
University Computing Regulations: University Computing Regulations (ed.ac.uk)	These regulations cover the use of all computing facilities administered on behalf of UoE.

5.4 UK LLC specific policies

Table 3 Bespoke UK LLC policies and SOPs that must be read, understood and followed by all UK LLC staff

UK LLC Policy/SOP Name	Brief Summary
Information Security Policy (POL-ISM-001) (This document)	Sets out UK LLC's approach to safeguarding the anonymity of individual participants, ensuring the security (confidentiality, integrity and availability) of the data stored in the UK LLC TRE and safeguarding legislative compliance.
Information Handling Policy (POL-ISM-002)	Details requirements related to the handling of UK LLC's information assets, including the data held in the UK LLC TRE and all the electronic files that comprise UK LLC's ISMS documentation.
Internal Roles, Responsibilities and Access Policy (POL-ISM-004)	Sets out the roles and responsibilities for the operation of UK LLC and the access to information that is required for each role.
*System Development Principles Policy (POL-DAT-005)	Details the secure engineering principles that must be defined and documented in all UK LLC projects that develop new systems or implement system changes.
Data Access and Acceptable Use Policy (POL-ISM-003)	Details the terms and conditions under which approved researchers access data held in the UK LLC TRE and UK LLC's commitments to LPS participants, data owners and researchers.
Reporting Weaknesses, Events and Incidents SOP (SOP-ISM-004)	Details the procedure UK LLC staff should follow to report any weaknesses in the UK LLC ISMS, as well as events and incidents.
Business Continuity Plan (DOC-ISM-009)	Details procedures to prevent or minimise (where possible) disruptions from occurring, and plans which are ready to continue delivering services when disruptions occur.

*This is a mandatory document for UK LLC Data Team ONLY

5.5 Incident reporting responsibilities and procedures

The responsibilities and procedures for reporting weaknesses, events and incidents, are detailed in the Reporting Weaknesses, Events and Incidents SOP (SOP-ISM-004). This SOP also covers evidence gathering and continual improvement.

6. RELATED DOCUMENTS

All policies and SOPs are available to all UK LLC staff on the UK LLC SharePoint: SOPs, Policies and Important Documents for UK LLC. All staff should be familiar with all UK LLC policies and all SOPs that are relevant to their business area.