UCL-IG16 Training Policy

Document Information	
Document Name	UCL-IG16 Training Policy
Author	Jack Hindley
Issue Date	31/03/2022
Approved By	Chair of IRGC
Next review	One year

Document History		
Version	**Date**	**Summary of change**
0.1	21/01/2013	First draft for discussion
0.2	24/01/2013	Incorporated feedback from Alice Garrett
0.3	24/04/2013	Revisions from Shane Murphy
0.4	10/06/2013	Incorporated revisions from Trevor Peacock
0.5	09/07/2013	Incorporated roles from IDHS-Roles-Workflow-and-Authorisation-Model-v3
1.0	02/08/2013	Approved by Chair of SLMS IGSG
1.1	21/08/2014	Amendments by Kristina Drew to reflect in-house SLMS IG training provision and simplified training requirements for SLMS job roles
2.0	23/09/2014	Approved by Chair of SLMS IGSG
2.1	23/03/2017	Reviewed by Jack Hindley
2.2	27/03/2017	Trevor Peacock's comments incorporated
3.0	29/03/2017	Approved by Chair of SLMS IGSG
3.1	23/11/2017	Reviewed by Jack Hindley
4.0	27/11/2017	Approved by Chair of IG Steering Group
4.1	15/10/2019	Updated to include references to DSP Toolkit; minor re-wording
5.0	22/10/2019	Approved by IGSG
5.1	03/06/2021	Added requirement for IAO training, changed SLMS references to UCL, references to 'staff' changed to 'team member'
6.0	09/06/2021	Approved by Chair of IG Steering Group
6.1	18/03/2022	Updated to reflect changes in the organisation
7.0	31/03/2022	Approved by Chair of IRGC

1. Purpose

UCL operates an Information Governance (IG) Framework in line with NHS Digital's Data Security and Protection (DSP) Toolkit in order to maintain proper handling of confidential information and for assurance on behalf of our external partner organisations in relation to, for example, sensitive personal data.

The DSP Toolkit requires that at induction and on an annual basis research team members must be made aware of local IG procedures, and in particular must be given clear guidance on their responsibilities. All UCL staff should receive GDPR training and be informed where to get more support and guidance. As per the DSP Toolkit, all research team members with routine responsibility for specific confidential information assets should receive additional annual training.

2. Scope

This policy applies to all research team members handling data in scope of the DSP Toolkit, including contracted, non-contracted, temporary, honorary, secondments, agency, students and volunteers.

3. Policy

3.1 Training Needs Analysis

The IAO must complete and maintain their own IG training. The IAO will ensure that all team members are annually reminded of procedures, policies and guidance, as advertised on the IG Approved Documents List (https://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/approved-documents).

Training for research team members who have responsibility for specific, confidential information assets must consistently and measurably cover all appropriate topics including information security, data protection and confidentiality.

Examples of appropriate training for staff are found in Appendix 1 of this document.

Research team members with responsibility for specific, confidential information assets should also be made aware at induction and on an annual basis where to find and how to comply with specific contracts governing the use of specific information assets where those exist.

Where a research team member with responsibility for specific, confidential information assets is unable to fully take part in appropriate information governance training with their employing organisation, appropriate external IG training will need to be sought by Information Asset Owners (IAOs).

UCL must continue to mitigate the risk of a breach of confidentiality by providing a high standard of training for research team members.

The content of IG training aims to ensure:

- that research team members in scope of the DSP Toolkit will operate in compliance with its requirements;
- that those with responsibility for specific, confidential information assets are given training and assessment appropriate to the type of information involved; and
- that team members are provided with training on local procedures that support the UCL IG Framework.

All IAOs must ensure team members are trained in accordance with this policy:

- during induction
- when a change in role and/or responsibilities occurs
- as part of an annual review

In carrying out the Training Needs Analysis, staff competencies should be compared against the job role requirements to identify training needs.

The IG Lead, with the approval of the Information Risk Governance Committee (IRGC), may also require that additional IG training is undertaken by research team members as a result of a security breach involving information assets.

When an unmet IG training need is identified, the IG Training and Awareness service will ensure that additional training for the role is made available.

3.2 Responsibilities

3.2.1 The UCL Information Governance Training and Awareness service will:

- Issue prompts and updates to research team members via email, meetings and newsletters regarding completion of annual mandatory IG training.
- Communicate how to access and to complete the required training.
- Monitor completion of IG training.
- Escalate cases of non-compliance via individuals' line managers and ultimately to the Senior Information Risk Owner
- Issue regular reports showing progress for IG training to the Information Risk Governance Committee members for discussion. The reports will be statistical only (no personal data) and obtained from the IG training register.
- Provide ad hoc reports to IAOs for monitoring performance of IG training. The reports will provide detailed information for IAOs' team members and will show completion of IG training.

3.2.2 IAOs are responsible for:

- Completing their own training, as detailed in 3.1 above.

- Completing a Training Needs Analysis annually for all research team members as in 3.1 above.
- Confirming and monitoring that their research team members have completed appropriate annual IG training
- Agreeing actions and associated timescales with research team members who have not completed appropriate training.

3.2.3 Research team members are responsible for:

- Completing appropriate IG training within a reasonable timescale during and after induction.
- Keeping themselves informed about changes to IG procedures and policy.
- Notifying their line manager when they cannot complete appropriate IG training within a reasonable timescale after induction.
- Refreshing their training annually according to their current Training Needs Analysis.

Appendix 1

Information Governance Training:
Specific training to be undertaken by research team members.

1. IAOs should ensure all team members are made aware during induction and reminded at least annually of local IG procedures and policy, as advertised on the IG Approved Documents List: https://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/approved-documents, and of where to find further support and guidance through the Information Governance web page: https://www.ucl.ac.uk/isd/it-for-slms/information-governance-and-research-facilitation

2. All research team members with responsibility for specific, confidential information assets, including the IAO, **must** attend appropriate information governance training which can be measured consistently and covers information security, data protection and confidentiality, either through the UCL IG Training and Awareness service or through a suitable external provider, e.g. an NHS Trust.

   NHS Digital's course, entitled *Data Security Awareness Level 1*, is available online to all UCL staff through the UCL IG Training and Awareness Service and provides appropriate training for staff working with confidential information. Once registered, staff need to complete four essential modules and pass an assessment after each.

   Research team members with responsibility for specific, confidential information assets should also be made aware at induction and on an annual basis where to find and how to comply with specific contracts governing the use of specific information assets where those exist.

3. Annual Refresher Training: research team members are required to re-take and successfully complete an appropriate IG training course each year. As part of this process staff will be directed to relevant IG training resources.

   - Individuals will be contacted by the IG Training and Awareness Service at least one month before their IG training is due to expire
   - Individuals will be required to re-take and successfully complete an appropriate IG training course before expiry of their current IG training
   - Those whose IG training lapses will be removed from the IG training register. The IG Training and Awareness Service will monitor training completion and will escalate any failure to renew via the team's IAO and ultimately the Senior Information Risk Owner.
   - Once expired, completion of appropriate IG training will be required before the team member can be granted access to the Data Safe Haven.

3. The training needs identified for each role will be mandatory and must be undertaken within six weeks of the role being allocated and every year thereafter.

4. Particular roles are required to attend specialist IG training sessions which will be operated by the IG Training and Awareness service:
    - Senior Information Risk Owner
    - IG Lead
    - Members of The IRGC
    - IG Service Owners
    - IG Service Operations Managers