# ScHARR IG Learning Needs Analysis Strategy v2

## This version (v2.0) approved IG Committee 2021-05-25

### Purpose

The learning needs analysis (LNA) seeks to identify skills and knowledge gaps in relation to data security and protection within ScHARR. This information can feed into the development of ScHARR's information governance (IG) policy and help to ensure that the training is tailored appropriately.

### Responsibilities

The development and agreement of the LNA is a joint task for members of the ScHARR IG Committee, with the Senior Information Risk Officer (SIRO) taking overall responsibility for the LNA and associated timescales.

### Scope

The ScHARR IG Policy applies to all those within ScHARR who receive, store, process or have any other form of contact with data collected for use in, or produced as a result of, research projects. As it is possible that anyone in the department may encounter sensitive information, all ScHARR staff (including Emeritus, Honorary, Visiting, seconded and short-term contract staff) and students must be familiar with the policy. The LNA thus needs to consider the training and learning requirements of these individuals.

Additionally, the LNA must consider the training and learning needs of the IG Committee itself, so that the individuals responsible for agreeing and promoting the policy are appropriately qualified for the role, and so that collectively the committee has the required knowledge and experience to meet ScHARR's IG needs.

### Process

#### *Selection and training of IG Committee members*

The IG Committee must simultaneously have suitable knowledge and experience of the issues around data protection and security while also representing ScHARR research interests. The structure of the committee and the associated role descriptions have been developed to ensure it is composed of individuals with significant experience of working with health data and/or the practical and ethical issues which must be addressed. It also includes representation from ScHARR DS, and an adviser on information security and compliance from a member of the University's Information Security team.

Members of the committee regularly attend meetings of the NHS/HE Information Governance Working Group, and subscribe to the mailing list.

A regular review of external training courses and materials is undertaken to provide relevant additional training where appropriate, in order to stay up to date with guidance and regulations regarding information governance.

*Training for ScHARR staff*

The committee has developed an online "ScHARR - Information Governance" training course to reflect the policy and to supplement the central University courses ("Protecting Information", "Protecting Personal Data", "Protecting Research Data", “Cyber Safety”).

All five courses must be completed before individuals are granted access to the data, files, servers and systems required to carry out their duties.

*Training for (non-ScHARR) collaborators*

It is expected that collaborators from outside of ScHARR (typically from the NHS or other academic institutions) will have completed equivalent training at their host organisation. However, it is mandatory that everyone additionally undertake the "ScHARR - Information Governance" module before being granted access to any risk-bearing data.

*Requirements for accessing third-party data obtained via DSPT*

If data is obtained using the Data Security and Protection Toolkit (DSPT) as the security assurance (e.g. NHS digital data, Public Health England data, data obtained via Section 251 approvals), access to this DSPT-assured data will be granted only to members of the University of Sheffield project team who have completed all five training modules as well as the University’s Assured Computing training, and have confirmed they are compliant with Cyber Essentials plus (CE+). Further sharing may be possible under other governance arrangements outlined in the data sharing agreement.

*Review and update of training materials*

The content of the training is regularly reviewed and updated in line with ScHARR IG policy, and in response to IG queries and incidents. ScHARR staff or collaborators may be required to carry out other applicable training as mandated by the ScHARR IG Committee.

| Version | Effective Date | Summary of changes |
|---|---|---|
| 1.0 | 18-Jun-2020 | n/a first version |
| 2.0 | 25-May-2021 | Addition of Cyber Safety training |