Information Asset Owner (IAO) for ScHARR NHS DSPT assured projects

This version (v1.0) approved by the IG Committee 2021-05-25

The ScHARR Information Governance Lead is responsible for data security and protection within ScHARR. The Information Asset Owner (IAO) is accountable to the ScHARR Information Governance Lead for managing the risks associated with handling risk-bearing information.

The IAO Is responsible for the information they control. This is at a local level, e.g. within a study, this is typically the Principal Investigator (PI) defining how research data is managed/processed for their specific project. The IAO must be a UoS employee, not an Honorary.

The IAO is responsible for ensuring that information processing adheres to relevant policies and procedures (UoS, ScHARR, and any special constraints, e.g. those demanded by the funder or data provider). If the PI is not employed by UoS then a staff member closely involved with the project will be the IAO.

Responsibilities of the Information Asset Owner

The Information Asset Owner must ensure:

- Data they are responsible for is stored in accordance with the agreements under which it has been provided and all Contractual requirements, relating to data in use by the study, are met (special attention must be given to ensure data storage and computing resources that are compliant with UoS Cyber Essentials Assured Computing are used where the DSPT is provided as a security assurance).
- Data sharing agreements (DSA) (if applicable) are signed by a member of the contracts team in research services (ri-contracts@sheffield.ac.uk).
- If not otherwise specified data are stored on a virtual machine or in an access restricted folder on the University's Shared networked Filestore (for which they will be the Primary Folder Administrator).
- There is a legal basis for holding personal data.
- All onward sharing of data is legal.
- Appropriate data processing contracts are in place where external parties are processing personal data on behalf of UoS.
- A data management plan (DMP) has been created and is implemented which covers the above points.
- Access is only granted to authorised users and access is removed for movers and leavers (for leavers the leavers checklist will be followed).
- Any requests for information regarding data and access are responded to promptly (e.g. emails from ScHARR IG, ScHARR DS or IT Services colleagues regarding the

management and administration of data, asset registers and folders for which the administrator is responsible).
- Any requests from ScHARR-IG for information related to the asset register are responded to promptly (e.g. requests for copies of DSAs, data flows, DMPs; details of where data is stored, who has access; details of their training; details regarding use of mobile devices and details relevant to IT Services Assured Computing).
- a new primary administrator is nominated should they leave ScHARR or otherwise seek to relinquish the “primary administrator” role.
- The data / folder is deleted or archived (see below) when no longer required.
- They have read the ScHARR information Governance policy and maintain their Information Governance training.
- They comply with all aspects of the ScHARR IG policy.
- Incidents are reported promptly.
- A Privacy Notice is in place where required.
- Subject Access Requests are handled in accordance with University guidance.

In addition, the IAO should ensure that all members of the study team understand their responsibilities. In particular, team members must receive Information Governance training before being given access to personal data. See also the Process for the management of ScHARR resources on the University shared filestore.

Adapted from
Information Asset Owner ('Owner') | Information Services Division - UCL – University College London