**St George’s, University of London**

**Research Information Governance Audit Process**

# **Background**

## The University has a legal duty to maintain the confidentiality, safety, security and integrity of all personal data it holds and disseminates. This duty is defined through the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018) and common law duty of confidentiality.

## The University in its capacity as either a data controller, or on behalf of other organisations as a data processor, handles confidential information to support a wide variety of projects across its research institutes. Therefore, where personal data is involved the University must ensure the confidentiality, integrity and availability of the data.

## An internal audit report, carried out by KPMG in 2019 identified that the University had no clear plan for data privacy and data asset audits for research projects, and a lack of oversight regarding the number and nature of ongoing research projects, the data retained and how this is managed.

## Acting on the findings from the report it was agreed that due to the scope of this work that a percentage of research projects handling personal data would be audited annually. The audits will purely concentrate on the information governance (IG) aspects of a research project and does not replace specialist audits covering clinical trials, research study, service evaluation or any other audits managed by the JRES.

## The aim of a research information governance audit (RIGA) is to provide assurance to the University on compliance of research projects with the University’s information governance policies and procedures.

# **The Audit Team**

## Though responsibility for research projects rests with the Institute Directors, in their role as Information Asset Owners (IAO), it was agreed that initially RIGAs would be carried out by an audit team led by the Director Information Services (as Senior Information Asset Owner) and involve the Head of Information Governance and the respective Institute Information Governance lead.

## The audit team may include Subject Matter Experts from other areas (e.g. Data Protection Officer, Head of IT services etc) within The University to ensure the necessary balance of expertise and competence.

# **Selecting a Research Project for Audit**

## A research project can be selected for audit:

* by an Institute Director
* randomly
* following a request by an external Data Controller whose data is being processed
* by a request from the project sponsor

# **Audit Scope**

## The audit scope will cover five areas of a project these are:

* IG project controls
* data management and location
* access management
* data disposal
* training and awareness

## The audit will seek to determine whether the project is adhering to, or could adhere to, the University’s IG Policies and Procedures.

## The audit may also involve any data processor or third party engaged by the project to ensure that a complete understanding of the handling of the data is obtained. The above checks will also apply to such parties.

## The audit team may request a tour of the locations where data is being processed / stored.

# **Documents the Audit Team will want to see**

## Prior to the audit, relevant documentation / evidence shall be submitted to the audit team. A documentation checklist, enclosure 1, will be provided for completion by the project Principal Investigator or identified lead.

## These documents / evidence will be used to supplement and inform the audit and will be reviewed by the audit team prior to the audit interviews. A finding may be included in the audit report when documents / evidence are not provided prior to the audit interviews without a reasonable justification.

# **Audit Interviews**

## The audit team will conduct an evidence-based assessment of the project controls and environment where data resides. The audit team will then undertake interviews of relevant staff (primarily the Principal Investigator or identified lead), review documents, records and uses of data along with an inspection of implemented controls.

## The audit team will make and retain notes from interviews, observations and testing. Copies of any documentation not supplied prior to the audit interviews may be requested for review by the audit team.

## The audit team will hold a closing meeting with the Principal Investigator or identified project lead to discuss the identified findings. The findings will be caveated if pre-existing material still need to be provided.

## The audit team may conduct a further review of its notes after the closing meeting, which could identify new findings. New findings will be communicated to the Principal Investigator or identified project lead.

## Any finding identified during the audit and corrected by the Principal Investigator or project lead prior to the closing meeting will be referenced in the audit report together with an acknowledgement that the issue was corrected.

## The audit team may request pre-existing evidence that was unavailable during audit interviews to be supplied within five working days of the closing meeting.

## If any issues of a serious nature are identified during the audit, then the audit team will raise its concerns with the Principal Investigator or project lead and appropriate Information Asset Owner immediately.

# **Definition of findings**

## The overall audit finding will be classified according to one of the University’s internal risk assurance ratings:

### Significant assurance

### Significant assurance with minor improvements

### Partial Assurance with improvements required

### No assurance

## Recommendations made during the audit will conform to the internal risk recommendation ratings score:

## high,

## medium,

## low.

# **Draft report**

## A draft audit report will be issued to the project lead.

## Although the audit team will consider all of the areas within the scope of the audit, the report may also identify areas of good practice demonstrated by the project.

## The Principal Investigator or project lead will be requested to check the draft audit report for factual accuracy and for project confidential and security sensitive information.

## The audit is based upon a sample of the project activities, as observed by the audit team. Therefore, the findings detailed in the audit report may not include all possible nonconformities which may exist.

## The Lead Auditor will email the final audit report to the Principal Investigator or project lead and IAO.

## Any recommendations contained in the report the project lead will be requested, with the agreement of the IAO, to complete an action plan which address all the recommendations.

# A**ction resulting from an audit**

## Findings that present a serious divergence from the University’s IG Policies and procedures or findings which present an unacceptable risk to the University will be addressed with the Information Asset Owner directly, and if required, by the University Data Incident process.

# **Issues and concerns**

## If the Principal Investigator or project lead has an issue or concern with any aspect of the audit process then the issue should be raised directly with the Senior Information Risk Owner as the lead auditor.

Enclosure 1: RIGA Checklist

**Enclosure 1**

**St George’s, University of London**

**Research Information Governance Audit Checklist**

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Name / Descriptor** |  | **DPIA completed** | Yes / No |
| **Institute** |  | **Privacy Notice** | Yes / No |
| **Project Lead** |  | **Information Asset Register** | Line number: |
| **Project Start** |  | **Audit Date** |  |
| **Personal Data Held** | Yes / No | **Information Governance Audit team** |  |
| **Data Classification** | Identifiable / anonymised / pseudonymised |

|  |  |
| --- | --- |
| **Document / Evidence Required** | **Documents / Evidence Provided** |
| **Project Controls** | |
| Is SGUL the Data Controller / Data Processor  (If a Data Processor who is the Data Controller?) |  |
| Who have key responsibilities for the project? |  |
| Who has access to the data |  |
| **Data Management and Location** | |
| Data flow diagram / descriptor |  |
| Format | Digital / Paper / Digital & Paper |
| Where the data is held – Digital Hardware (Network drive, Laptops, Drives, memory sticks etc) |  |
| Where the data is held – Digital Software (Databases, software applications) |  |
| Where the data is held - Paper |  |
| What is the disaster recovery plan (back-up etc) if data not located within a University network drive? |  |
| Is the digital hardware supported by the University IT services? If not, then by whom. |  |
| Confirmation that a contract / data sharing agreement with third parties who have access to the data is in place. |  |
| **Access Management** | |
| How are data access permissions given or removed? |  |
| How is physical access to project locations managed? |  |
| What controls are in place for digital data e.g. password, encryption etc |  |
| **Data Disposal** | |
| Project end date: |  |
| What is the data retention period for the project data? |  |
| How are / will assets be disposed of? |  |
| **Training and Awareness** | |
| Have all staff involved with access to the data completed their mandatory DPA and Information Security awareness training.  (Names and dates required.) |  |