Information Governance (IG) aims to safeguard data in a continually changing environment. Policies which cover IG need to evolve in line with these developments and therefore the ScHARR IG Policy will be updated as necessary on these web pages. Although printable copies of this policy is provided for ease of reading, it should not be saved by the reader as either paper or electronic copy on a local or shared network drive. Staff and students will be notified by email when a new or revised policy is published.

# *ScHARR Information Governance Policy*

# *Overview*

A robustly constructed Information Governance (IG) framework allows an organisation to ensure that information is processed in accordance with all applicable regulations and guidance, such as the General Data Protection Regulations (GDPR), the Human Rights Act and the NHS Caldicott principles. The framework details the requirements, standards and best practice according to which information should be handled. Information should be managed securely and efficiently, and appropriate policies, procedures and management accountability should underpin the principles of the IG framework.

ScHARR's IG policy is predominantly concerned with the handling of information related to research projects and research participant data, particularly that which is personal, confidential or sensitive. All research projects handling personal data should have a data management plan (DMP) which should address data capture, integrity, confidentiality, retention, sharing and publication, as per the Research Data Management Policy[1].

It is ScHARR's policy to store only the minimum personal data required to satisfy the purpose for which it is collected, i.e. only anonymised or pseudonymised data is collected and stored where feasible. All research involving human participants, personal data or human tissue must be reviewed via one of the routes outlined in the University of Sheffield Research Ethics Policy[2]. In addition, individuals have a right to be fully informed about all aspects of a research project in which they may participate, outlined in The University of Sheffield Ethics Policy note 2[3]. Additional important information about data processing and legal rights of research participants is available through the University's Privacy Notice[4].

IG within ScHARR is under the direction of the ScHARR IG Lead; the ScHARR IG Committee takes responsibility for ensuring tasks and activities relating to IG are carried out. Current membership, Terms of Reference of the Committee and role descriptions of the members are available on the ScHARR IG webpage[5].

# *Definitions*

**Data**: For the purposes of this ScHARR policy data includes both information about research participants and documentation related to research work.

**Risk-bearing data**: Personal, sensitive or confidential data about individuals, or information that is otherwise sensitive (e.g. commercially or politically sensitive information). The loss of risk-bearing data could be detrimental both to any individuals who might be identified and to the University's reputation.  Pseudonymised data, where names and other personal identifiers have been replaced by a unique code, are still considered risk-bearing.

[1] https://www.sheffield.ac.uk/library/rdm
[2] https://www.sheffield.ac.uk/rs/ethicsandintegrity/ethicspolicy/approval-procedure/routes
[3] https://www.sheffield.ac.uk/rs/ethicsandintegrity/ethicspolicy/policy-notes/homepage
[4] https://www.sheffield.ac.uk/govern/data-protection/privacy/general
[5] http://www.sheffield.ac.uk/scharr/research/igov/committee

**Information assets**: Information assets include all research generated data, whether personal, sensitive or otherwise, along with associated documentation, hardware, software and any systems used in the pursuit of research aims.

**Information incident**: An information incident is a potential or actual breach of data confidentiality, security or information governance policy.

**Members of ScHARR**: For the purpose of this policy members of ScHARR include Honorary and Visiting staff, secondees, students and external researchers holding Service Level Agreements with the School as well as those on the University payroll.

**University-managed devices**: devices running YoYo or managed desktops, e.g. desktops and laptops.

# *Purpose*

The purpose of this policy document is to ensure that members of ScHARR understand their responsibilities in the management of research data and associated information assets.

# *Scope*

Each member of ScHARR should be familiar with the principles and practices outlined in this policy document. All research should be conducted in accordance with this policy.

# *Policy review and update*

The IG Committee will undertake regular reviews of ScHARR's IG policy to ensure that it remains up to date and fit for purpose. The Committee will incorporate findings of any information incident investigations and requirements of outside agencies into this reviewing process and update policies and practices as necessary.

# Section 1: Training and compliance

## Background

Each member of ScHARR, whether or not they carry out research, is likely to come into contact with the risk-bearing data. All members of ScHARR will be provided with appropriate IG training, which they must complete to register their compliance.

The IG Committee will be responsible for the oversight of training needs with annual review to determine the overall scope and shape of that training.

Each member of ScHARR is required to complete IG training.

## Policy

### Training and support

Each member of ScHARR must complete the mandated IG training as advised by the ScHARR IG Committee. This includes both the University-wide training[6] and the ScHARR-specific training module[7]. Any member of ScHARR who will have access to data that relies on the Data Security and Protection Toolkit (DSPT) as the security assurance (this may include data from data providers such as NHS Digital and data processed with Section 251 approval) must work within the University's Cyber Security Assured Computing framework. As such, they must carry out Cyber Essentials Assured Computing training[8] and any further training as mandated by the ScHARR IG Committee.

University data security training consists of three modules (Protecting Information, Protecting Personal Data, Protecting Research Data), ScHARR requires these to be repeated annually. The ScHARR-specific training module (ScHARR - INFORMATION GOVERNANCE) and Cyber Essentials Assured Computing training must also be completed annually.

Where third party workers have access to risk-bearing data under the control of the UoS they must complete the ScHARR-specific training module and any other training required to ensure compliance with any security assurances given to data providers, e.g. through the Data Protection and Security Toolkit (DPST), data sharing agreements or contracts. This means, for example, that third party workers who rely on the DSPT as the security assurance must undertake and be compliant with the Cyber Essentials Assured Computing training.

The ScHARR IG Committee will maintain a register of IG training completed by members of ScHARR.

[6] https://infosecurity.shef.ac.uk/
[7] https://infosecurity.shef.ac.uk/training_courses/online/scharr-information-governance
[8] https://infosecurity.shef.ac.uk/training_courses/online/assured-computing

## Policy enforcement

Failure to undertake appropriate IG training will result in suspension of access to University services (email, Google drive, calendar and Networked filestore folders) in line with the Procedure for overdue IG training renewal[9] .

Each member of ScHARR should be aware that failure to abide by ScHARR's IG policies may result in disciplinary action being taken against them. Repeated or persistent infractions should be referred by the relevant Section IG Lead to the individual's line manager or supervisor for action. Escalation to more senior management will occur should there be continued failure to comply with the School's IG policies.

[9] https://drive.google.com/file/d/1-D7UVV6qVRTIwlLCHgMg54KPfneXYSCE/view

# Section 2: Information assets management

## Background

It is the duty of the School, through its IG management processes and structure, to be aware of and safeguard the information assets it possesses. The primary objective is to ensure that, in the event of damage, destruction, loss or theft, there is awareness of what information is affected and, in the case of loss or theft, whether the information held on the asset is protected from unauthorised access.

## Policy

Each member of ScHARR must manage all of their data in a way which satisfies legal and ethical obligations regarding patient confidentiality.

ScHARR must maintain a register of information assets. In practice there are three registers:

- a hardware inventory register, maintained by The Faculty IT Hub, listing each item of hardware used to record or store data (including audio/visual equipment), against the individual to whom it is assigned and details of its destruction if applicable. To enable the hardware inventory register to be kept up-to-date, hardware must be purchased through The Faculty IT Hub, and line managers must complete a leavers checklist[10] with any staff leaving ScHARR.

- a register of all projects maintained on the University's Shared Networked Filestore, also maintained by the ScHARR Data Security team (ScHARR DS), detailing the project name, folder location, folder administrators, which users have access, and, if applicable, the expected archival/deletion date. Folder administrators are responsible for approving access. The leavers checklist is used to ensure access is removed when staff leave ScHARR.

- a register containing details of all projects using the Data Security and Protection Toolkit (DSPT) as the security assurance, including project title, the information asset owner (usually the project lead), dates that the data sharing agreement is applicable between, details of data location and medium, and data destruction details. The IG Committee will keep the DSPT as a security assurance asset register up to date.

[10] https://www.sheffield.ac.uk/scharr/staffinfo/hr/policies#leaving

## Device (hardware) management

All IT facilities (hardware, software, data, network access, third-party services, online services or IT credentials) provided or arranged by the University of Sheffield must be used in compliance with the University of Sheffield's IT Code of Practice.

It is expected that both personal and University-supplied portable devices (e.g. laptops, tablets, mobile phones, removable hard-disk/solid-state drives, USB drives) and personal desktops may be used off campus for work purposes with appropriate safeguards in place and subject to any other applicable agreement; refer to policy section 3 "Data storage and storage devices" and policy section 4 "Remote working".

University desktops are not expected to be taken from UoS premises, unless such removal has been authorised. If University desktops are to be taken off campus (e.g. to be used at home) then, in addition to safeguards described within policy section 3 "Data storage and storage devices" and policy section 4 "Remote working", the following safeguards must be in place::

- the equipment is encrypted (this must be checked with The Faculty IT Hub);
- the equipment location is kept up-to-date on the Faculty hardware inventory register;
- (if staff are not returning to work) a process is in place to return equipment, e.g. the leavers checklist must always be completed.

### Device users

#### University-owned devices

Any device purchased by the University is owned by the University.

Devices must not be used by individuals who are not members of ScHARR unless under the direct supervision of a member of ScHARR at all times (e.g. an external guest using a ScHARR computer to give a presentation to members of ScHARR). University-managed devices may be used by other members of ScHARR provided each user uses their own university account (consent should be obtained from the individual to whom the device is assigned or from their line manager or Section Manager). Devices which are not University-managed must only be used by the individual to whom the device is assigned.

If the primary user of a University-owned device changes, the device must be wiped and reimaged and the Faculty IT Hub must be informed in order to update the hardware inventory register.

#### Non-University devices

See policy section 4 "Remote working".

### Device disposal / primary user leaves ScHARR

#### University-owned devices

Once University equipment has reached the end of its useful working life, it is expected that the equipment will be returned to the Faculty IT Hub for secure disposal and the asset register updated with details of the destruction certificate.

When a member of ScHARR leaves the University or ScHARR, it is expected that all University-owned devices in their custody will be returned to their line manager or Section Manager for them to arrange secure reassignment (including wiping and reimaging) or disposal, and to notify the Faculty IT Hub so that the asset register can be updated.

**Personal devices**

Before disposing of- or providing access to- personal devices which have ever been used for University work/study purposes, members of ScHARR must ensure:

- all risk-bearing data (if any) has been securely erased
- all access to University systems has been removed (e.g. revoked access to University Google account for all Apps)
- credentials relating to University systems have been securely erased (e.g. login details; VPN connection settings, etc.).

A “factory reset” including the deletion of all user data is strongly recommended.

Upon ceasing to be a member of ScHARR, individuals must ensure all personal devices which have ever been used for University work/study purposes have:

- all risk-bearing data (if any) securely erased

ll waste IT equipment will be collected and disposed of by The Faculty IT Hub in accordance with the University’s procedure for the disposal of waste electrical and electronic equipment[11] (WEEE). The Faculty IT Hub will update the asset register.

[11] https://www.sheffield.ac.uk/efm/recycling-waste/confidential-waste

# *Section 3: Data storage and storage devices*

## *Background*

ScHARR stores large volumes of research data, some of which is risk-bearing.The wrong choice of storage could put research work at risk of unauthorised access or loss and could damage the University's reputation.

In order to choose appropriate storage the following issues should be considered:

- **security** - ensuring that data is protected from unauthorised access. This is particularly important when working with risk-bearing data
- **availability** - ensuring that data is accessible when and where it is needed
- **integrity** - ensuring one true copy of the data is maintained.

## *Policy*

Data from each research project should be stored in accordance with the agreements under which it has been provided. It is recommended that risk-bearing data are stored in an access restricted folder on the University's Shared Networked Filestore, only accessible to approved users. Where this is not practical, alternative or additional secure data storage must be chosen based on an assessment of potential risk. Advice must be sought from the relevant Section IG Lead.

### University network storage

ScHARR DS will create secure folders with controlled access and arrange archive or deletion on request. This will be documented in an information asset register.

For each project folder, research groups must only request access for those individuals who have a definite need for access to the contents of that folder. There is provision for secure access for people outside of the University when necessary. A member of the research group must notify ScHARR DS promptly when a member of staff no longer needs access.

IT Services manage the regular backup of all University file storage for disaster recovery purposes.

### Google Drive

The University has an agreement with Google for provision of G Suite (Google Apps). The Factsheet on Data Security and Privacy with Google[12] summarises this agreement and states that the University is satisfied that the security controls put in place by Google are sufficient to protect University data. This applies only to University-supplied Google accounts and not personal ones.

[12] http://www.shef.ac.uk/it-services/google/security

Google Drive may be used by research groups as a tool to develop documents and spreadsheets collaboratively. However, it is not recommended for use as a project's primary data storage for a number of reasons:

- when a Google account is deleted any documents owned by that account are also deleted unless they are first transferred to another account
- back-up and disaster recovery procedures are managed by Google and therefore not within the control of IT Services
- there is increased risk of accidentally sharing data inappropriately
- users might have granted third-party applications (which may not have been formally assessed) access to files within Google Drive
- using Google Filestream (which is endorsed in University guidance) could lead to files stored on Google Drive being copied onto a local machine (which would not be compliant with ScHARR IG policy).

For these reasons Google Drive should not be used for risk-bearing data without very careful consideration of risks, and consultation with and approval from the appropriate Section IG Lead. When making these decisions consideration must be given to the regulatory (GDPR) requirements to maintain an asset register and to monitor access and training. Specific processes would need to be put in place: to document granting and removal of access; to ensure files are only accessible to individuals who have completed the relevant training; to ensure access is removed when individuals leave the organisation; to document the expected archival/deletion date; and to inform the Section IG Lead where this information is maintained in order to be referenced by the register of all projects which must be maintained by ScHARR.

If the decision is made to collect or store risk-bearing data using Google Drive, e.g. via Google Forms, then this should be made clear to study participants.

Google Drive must not be used to store data that relies on the DSPT as the security assurance.

## High Performance Computing (HPC)

As part of its research computing[13] offering, IT Services offer high performance computing services (e.g. ShARC and Bessemer) for work requiring intensive computational resources. These should not be used for processing risk-bearing data without first consulting your ScHARR IG lead.

## External services

External services should only be used for storage or processing of risk-bearing data following very careful consideration of risks.

Examples of external service providers include:

- cloud storage services such as Dropbox, iCloud, OneDrive and Google Drive on personal (non-University) Google accounts
- online survey services such as SurveyMonkey (and Google Forms on non-University Google accounts)
- chat and video conferencing services (e.g. Slack, Zoom)

[13] https://www.sheffield.ac.uk/it-services/researchcomputing

- agencies which process data (eg mailing, transcription)
- agencies which develop/maintain IT systems to support research projects

If a research group is considering using an external service for something which involves the processing or storage of risk-bearing data, they must consult the IG Section Lead for advice. If it is agreed that the use of an external service is appropriate, a contract must be in place to ensure there are sufficient security measures and compliance with the General Data Protection Regulations (GDPR).

## Data from third party providers

There may be further restrictions placed on data received from third party providers, for example:

- storing and processing data only on University premises
- storing/accessing the data only on a computer with no internet connection
- storing/accessing the data only using encrypted machines
- preventing off-campus access
- preventing download from primary storage
- encrypting data to a specific minimum standard
- applying additional firewall restrictions
- securely deleting files by an agreed date or at the request of the provider
- documented destruction of hardware at end-of-life

Data sharing agreements (DSA) will document any restrictions which must be adhered to.

In some cases using a virtual machine (VM) may be an option to meet the requirements of a DSA. IT Services maintains the physical infrastructure, and access to a particular VM can be restricted to specific user accounts. A firewall can be configured at VM-level to permit connection only from specified IP addresses, and data transmissions to and from the VM are encrypted by Transport Layer Security (TLS). Requests for VMs should be made via IT Services, and the IG Section Lead must be informed.

### Data Security and Protection Toolkit (DSPT)

If projects rely on the DSPT as the security assurance (e.g. DSPT has been referenced in the project's ethics application or within a data sharing agreement), the IG Section Lead must be informed so that details can be logged on the DSPT as a security assurance asset register.

Data storage and processing of this data must be undertaken within the University's Cyber Security Assured Computing framework[14]. Working within this framework allows us to demonstrate compliance against a range of data security standards that are required by the DSPT.

This Assured Computing framework restricts where data can be stored and on which types of machine that data can be processed. Although Assured Computing allows data to be stored on Google Drive, for DSPT assured projects, **only the University network storage may be used** (i.e. the X: drive, or the drive that maps to the University network storage that is accessible from an IT ServicesVirtual Machine). Google Drive must not be used to store DSPT assured data .

[14] https://www.sheffield.ac.uk/it-services/assured-computing

The Assured Computing framework also requires that users have undertaken specific training[15].

If alternative security assurances to those outlined above are used these must be outlined within the project documentation, e.g. ethics application, any data sharing agreement etc and the DSPT must not be given as the security assurance.

### Data Sharing Agreements (DSAs)

Any DSA with an external body must be approved by an authorised signatory in Research Services. Requests should be directed to ri-contracts@sheffield.ac.uk for review and approval (see section 5).

## Storage on local hard drives / solid state drives

When performing process-intensive tasks it can be beneficial to work with data on a machine's local drive rather than a network drive. If the data being processed is risk-bearing, this is only acceptable where this does not violate a data sharing agreement, there has been a careful consideration of risks (documented within a data management plan) and the local storage is encrypted[16] in accordance with University policy[17]. It is recommended that local drives are used only for temporary storage (during processing) as they are vulnerable to corruption or failure, and are unlikely to have comprehensive back-up and disaster recovery plans in place. When performing tasks that need to comply with the Cyber Essentials Assured Computing standards (including any processing of DSPT assured data, which may include NHS Digital-provided data, data must never be saved on local hard drives / solid state drives.

## Portable devices

Portable devices (e.g. laptops, USB sticks, hard drives, voice recorders, mobile phones, tablets) should only be used for *temporary* storage of data (and only where this does not violate any data sharing agreement) as they are vulnerable to loss or corruption. If portable devices are used to store risk-bearing data or used to access information which could include risk-bearing data (including receiving and sending email), they **must** be encrypted. It is recommended that **all** portable devices used for work purposes are encrypted. Any device that is capable of receiving a work email (e.g. a phone) is therefore capable of downloading risk-bearing data, and **must** be encrypted before being used for this purpose.

## Audio / video recordings

Audio and/or video recordings should only be made on dedicated encrypted recording devices or as specified in the "Remote audio / video recordings" section, below. No other mobile/tablet apps, nor software or application extensions for any device, should be used for such audio and/or video recording unless they have undergone a risk assessment and have been approved by the ScHARR IG Committee. Alternative means of recording should only be

[15] https://www.sheffield.ac.uk/it-services/assured-computing/training
[16] Unlike straightforward password protection, which simply acts as a barrier to accessing the information, encryption renders information unreadable to anyone who does not have the right key/password.
[17] http://www.shef.ac.uk/it-services/encryption

used for research work following careful consideration of risks and consultation with the Section IG Lead.

## Remote audio / video recordings

ScHARR staff/students may make audio / video recordings using Blackboard Collaborate or Google Meet services under contract to the University of Sheffield (i.e. they must use their University accounts only) subject to the following general and service-specific conditions:

### General conditions

Before making any recording, staff/students making recordings MUST ensure:

- their PC or laptop conforms to the ScHARR IG policy
- they make participants aware that the security of the participants'/interviewees' device is the participant's responsibility and if they are concerned they should not say anything they would not otherwise say while using their device/phone
- meetings contain only the participant(s) expected, with special regard to telephone participants whose identities may be more difficult to verify
- they only record audio (unless there is a strong and documented need for video) by asking the interviewee to turn off video before commencing recording
- they do not inappropriately/inadvertently share the resulting recording(s)
- they, as soon as practicable, move the resulting recording(s) to a suitable longer-term storage location for “risk-bearing data” whilst observing the usual safeguards to ensure data is protected (see Section 3: Data storage and storage devices)
- they permanently delete the original recording(s) from Google Drive or Blackboard Collaborate and do not seek to recover the recording(s)

### Blackboard Collaborate specific conditions (only accessible to staff)

Before making any recording, staff making recordings MUST ensure:

- they set up a new 'Organisation' in Blackboard Collaborate with access restricted to members of the research team who require access to the recordings
- they create appropriate interview sessions within the access-restricted “Organisation” space defined above, ensuring any recordings made will only be stored within this space within Blackboard Collaborate
- the Blackboard Collaborate session setting to allow participants to download the recording is set to ‘disabled’
- the Blackboard Collaborate session settings for all participants is set to the minimum required, with special regard to the sharing of audio, video, post chat messages, draw on whiteboard, files

### Google Meet specific conditions

Before making any recording, staff/students making recordings MUST ensure:

- they have not granted any third-party (non- Google G Suite) apps access to their university Google Drive account (see https://myaccount.google.com/permissions)
- they do not "sync" or "stream" the contents of their university Google Drive account to any devices that do not conform with the ScHARR IG policy

**More information on remote audio / video recording**

University and Blackboard guidance on using Blackboard Collaborate sessions.

University and Google guidance on recording using Google Meet.

## Paper records

Research project staff should discuss their requirements with their Section Manager to ensure paper records are stored securely and archived/deleted when appropriate. Where necessary, the Section Manager will consult with the Records Management Team.

Information captured on paper is just as important as data stored digitally and carries many of the same risks, therefore care must be taken to ensure secure transit of anything containing risk-bearing information.

## Data disposal

The disposal of risk-bearing data requires particular care. Files which have been deleted in the usual way may still be recoverable; instead files containing risk-bearing data must be securely erased. ScHARR DS can provide technical assistance.

The retention period for research data is determined by guidance from regulators, funders, sponsors and data providers, which must be adhered to. The retention period must be clearly defined within the ethics application and data management plan. The University of Sheffield records retention schedule[18] can provide guidance if no other guidance is available. Risk-bearing data must be securely erased at the end of the retention period.

NHS digital has specific requirements to destroy NHS digital provided data at the end of the data sharing agreement (DSA). It is possible to retain appropriately anonymised or derived data (as allowed under the contracts governing the data sharing), along with analysis code and data extraction requests unless otherwise stated in the DSA. However, details must be provided in a data destruction certificate.

Further advice on data destruction should be sought from the ScHARR IG Lead.

[18] https://www.sheffield.ac.uk/polopoly_fs/1.821413!/file/2019_UoS_retention_schedule_rewrite_v2.3.pdf

# *Section 4: Remote working and working on devices which are not University-managed*

## *Background*

Working away from University premises and/or with devices which are not University-managed introduces additional risks, for example devices may be lost, damaged or stolen. Without appropriate protection this could result in the loss or inappropriate disclosure of risk-bearing data. Each member of ScHARR has a responsibility to protect risk-bearing information and the systems they use to store, process or access that information. Each member of ScHARR should be aware of the risks involved and take measures to safeguard the data. Losses of confidential data are viewed very seriously by the Information Commissioner's Office and the University, and may result in consequences such as disciplinary procedures, civil court actions and criminal charges.

## *Policy*

It is expected that most staff, the majority of the time, will work within the University environment on University-managed devices.

Any risk-bearing data accessed from- or stored outside- the University Shared Networked Filestore is protected (in transit and at rest) using an approved encryption system. Devices used to process - or which enable access to (e.g. using University VPN) - risk-bearing data must meet the following minimum standards:

- the data on the device must not be accessible to unauthorised users
- the device must run under a vendor-supported and up-to-date operating system with all security patches applied
- the device must have appropriate firewall rules enabled
- if using Windows, the device must run an up-to-date anti-virus application
- the device must be encrypted

When working off site take care that work on sensitive information cannot be overlooked.

There may be further restrictions placed on data supplied by third party providers, and data sharing agreements (DSA) must be adhered to in these cases.

More detailed guidance around working from home during the Coronavirus (COVID-19) pandemic is available[19].

[19] https://drive.google.com/file/d/1bUQ4tU1fURD1fqamabbLByp9KaLWvz5f/view

# Section 5: Information sharing

## Background

Researchers may have cause to share data relating to research participants with other persons, researchers or organisations. Sharing individual participant data can advance clinical research and benefit patients, but any sharing of data must always be in accordance with the law, and must be authorised under the agreements that govern the use of the data.

Data sharing and transferring requests must be handled in accordance with the requirements of GDPR and other relevant guidance, e.g. the NHS Caldicott principles. A failure to safeguard information could result in legal action.

Each member of ScHARR must at all times have great regard for the safeguarding of the research data in their possession. Smith et al (2015)[20] provides useful background information and guidance on data sharing and anonymisation and this is the document on which this ScHARR policy is based. If a person is unsure as to what action they should take then they should, in the first instance, approach their section IG Lead (Supervisor or Personal Tutor, in the case of students) and discuss the matter with them.

This policy must be applied to all information sharing requests that are not already authorised. This includes requests from individuals and groups both inside and outside of the University. For sharing of data outside the European Economic Area (EEA), please also see Section 7. Where sharing is already pre-authorised, e.g. with external collaborators, the project documentation should cover the IG arrangements for the other institution(s).

## Policy

There must be a clear purpose to share research data which is aligned with the purposes for which the data were collected. The project team should ensure a system is in place to review data access requests and only accept them if this is satisfied. Similarly, data should only be deposited with data repositories which follow these principles.

Consent must be sought from data subjects if it is appropriate and practicable to do so (although a lack of consent for sharing does not prohibit the sharing of data that is not reasonably likely to lead to the identification of individuals or if Section 251[21] approval has been obtained).

It is recommended that the following (or similar) wording be included in consent forms: “I understand that the information collected about me may be used to support other research in

[20] Good Practice Principles for Sharing Individual Participant Data from Publicly Funded Clinical Trials. Tudur Smith C, Hopkins C, Sydes M, Woolfall K, Clarke M, Murray G, Williamson P. April 2015.
[21] Section 251, accessing confidential patient information without consent

the future, and may be shared anonymously with other researchers." Other data providers may have their own preferred wording.

Individuals have the right to be informed about the collection and use of their personal data and must be provided with information including the purpose for processing their personal data, retention periods and who it will be shared with (i.e. 'privacy information'). It is important that this privacy information includes information regarding how to 'opt-out'; if using data from NHS organisations (using Section 251 approval), where direct identifiers will not be obtained, then this information will most likely be to direct potential participants to the national data opt-out policy. If collecting data directly from consented participants it should be included within the participant information sheet (PIS). The ethics application process should document how this privacy information will be shared. For data obtained from third parties, where Section 251 approval has been obtained, it is likely this information will be provided in the form of a privacy notice. If projects rely on the Data Security and Protection Toolkit (DSPT) as the security assurance (e.g. projects that require Section 251 approval), the IG Section Lead must be informed so that details can be logged on the NHS Digital / ScHARR DSA list asset information register and the privacy notice checked. Authorisation to share the information must be in place: agreement should be made within the project team regarding who should authorise requests for data sharing and it is expected that this will be outlined in a data management plan[22]. As a minimum this should be from the project lead, but may also include the sponsor and ethics committee. Roles and responsibilities should be included in the protocol and data management plan. Refer also to the University Research Ethics Policy guidance document regarding sharing with other researchers within the University (Internal data transfer principles and procedures)[23].

Data must be anonymised as far as possible prior to being shared. There may be a trade-off between privacy and data utility as it can be difficult to attain true anonymisation and it is difficult to predict the risk of re-identification through data linkage. Refer to the University's Research Ethics Policy Note no 4[24]. and Specialist Research Ethics Guidance Paper[23] (PRINCIPLES OF ANONYMITY, CONFIDENTIALITY AND DATA PROTECTION).

The recipient of information must agree to safeguard the security and confidentiality of risk-bearing data. Where the transfer is outside ScHARR an agreement must be in place as part of a contract or as a separate data sharing agreement (DSA). This should outline the purpose and security arrangements. For sharing with external institutions The University is generally legal party to DSAs to ensure that legal liability rests with the institution, rather than an individual employee/student.

Any DSAs with external institutions must be approved by an authorised signatory in Research Services, and enquiries should be directed to ri-contracts@sheffield.ac.uk for review and approval.

It is the responsibility of the person receiving or sharing the data (e.g. student or supervisor; member of a project team) to ensure compliance with all the obligations of the agreement on behalf of the University. Therefore the person receiving or sharing the data should sign the

[22] https://www.sheffield.ac.uk/library/rdm/dmp
[23] https://www.sheffield.ac.uk/rs/ethicsandintegrity/ethicspolicy/policy-notes/homepage (see other useful documents)
[24] https://www.sheffield.ac.uk/rs/ethicsandintegrity/ethicspolicy/further-guidance

document in acknowledgement of the terms and conditions as well as a member of the Research Services Contracts Team.

Example DSAs are given at the end of this section. The correct template to use will depend upon whether or not personal, pseudonymised or general data is being shared. It is important to be cautious with regards to how to categorise data, being aware of situations that could make data identifiable such as combinations of data, links to other available datasets, rare diseases, free text fields etc. Refer to the University's Research Ethics Policy Note no 4[23]. and Specialist Research Ethics Guidance Paper[23] (PRINCIPLES OF ANONYMITY, CONFIDENTIALITY AND DATA PROTECTION).

Risk-bearing data must be shared securely. Files must be encrypted before they are sent via e-mail or stored in locations other than the University's network drive. IT Services offers guidance on how to encrypt files[25]. Any difficulties should be discussed with the relevant Section IG Lead.

## *Example DSAs*

Personal data

Pseudonymised data

General data

[25] http://www.shef.ac.uk/it-services/encryption/protectingemails

# Section 6: Incident management

## Background

In order to protect sensitive information and to comply with both the data protection legislation (GDPR) and the incident management guidance made available by NHS Digital, it is vital that procedures are in place to report any potential breaches of data confidentiality and security, i.e. information incidents. Information incidents include cases where there is potential, as well as actual, loss of or damage to data.

Examples of information incidents include:

- Shared usernames and passwords. This is a breach of Information Security and expressly forbidden by the University. People may access more information than they are permitted to see, which is a breach of GDPR
- Computers that are not protected by a password or are left unlocked
- Computers with risk-bearing data stored unencrypted on the hard drive
- Offices left unlocked, or doors held open
- Lost/stolen equipment containing risk-bearing data that are not appropriately protected
- Information stored on external services without the proper checks
- Information shared incorrectly, e.g. transmission of risk-bearing data unencrypted by email
- Saving of usernames and passwords within web browsers of computers that are not protected
- Reuse of usernames and passwords

Potential information incidents will be assessed by the IG Committee. In cases where this initial assessment indicates that risk-bearing data has potentially been shared outside of 'trusted' partners, as defined in the guidance on reporting an incident for the Data Protection Regulation (GDPR) and Networks and Information Systems (NIS) Directive[26], this guide will be used to direct subsequent actions. A more detailed guide to the reporting procedure is available from the ICO web pages[27].

## Policy

The IG Committee will formally assess and document risks to information and the controls put in place to manage risk.

The IG Committee will work with ScHARR Research Ethics Committee (REC) to assess IG risk on projects considered by ScHARR REC[28].

Any suspected information incident must be reported to a Section IG Lead, the IG Manager or the School IG Lead as soon as possible.

[26] https://www.dsptoolkit.nhs.uk/Help/29
[27] https://ico.org.uk/
[28] www.sheffield.ac.uk/scharr/research/ethicsgovernance

If ScHARR staff become aware outside of normal working hours of an information security incident that involves a serious loss of risk-bearing data and/or damage to computer systems, they should report it to University Security on 0114 222 4085, as mandated in the Information Security Incident Policy and Procedure[29].

Once the IG Committee are aware of a possible information incident they will:

1. record the incident in an Incident Investigation Log
2. carry out an investigation to establish the details and assess the impact, including the nature of the incident, the type of data involved, the perceived sensitivity of the data and the number of people affected, and record the details in the incident log[30]
3. where the incident involves a serious loss of risk-bearing data and/or damage to computer systems, immediately inform IT Services according to their standard Security Incident Policy and Procedure
4. if illegal activity (for example, theft) is suspected, ensure University Security Services have been informed
5. document any corrective actions taken and preventative actions to be taken in order to attempt to prevent any recurrence of this type of incident

The Incident Investigation Log should only be shared outside of the IG Committee where necessary and at the discretion of the IG Lead, unless there is a legal requirement to do so.

Where the incident is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor the IG Lead should report this to IT Services; the named liaison with the ICO within IT Services will decide whether this needs to be reported to the Information Commissioner's Office, or other authorities, and raise the report as necessary. The IG Lead will ensure that the IT Services person who is the named liaison with the ICO is aware of data specific requirements and notification details (for example, to notify the data provider) and will ensure these requirements are also met.

[29] https://www.sheffield.ac.uk/it-services/policies/securityincident

[30] This assessment may involve other relevant staff, such as IT technicians if appropriate: it may be necessary to download, open, read, copy or move files in order to determine whether they contain risk-bearing data

# Section 7: International data transfers

## Background

In accordance with GDPR, any risk- bearing data  may not be transferred to locations outside the European Economic Area (EEA) unless the receiving organisation is in a position to guarantee the security rights of the data subjects to a satisfactory standard.

## Policy

In addition to the considerations listed in Section 6:

- Prior to any data transfer outside the EEA the Section IG Lead must be consulted.
- Depending on the complexity of the case it may be necessary to seek more detailed advice from the University's Research Services or from the Information Commissioner's Office.
- If the recipient country is not on the list of approved destinations it may be necessary to draft specific contractual guarantees with respect to confidentiality[31]. This should be dealt with on a case-by-case basis.
- Data that has been anonymised, or subjected to strong pseudonymisation, and cannot be further processed to recover identifiable information, may usually be transferred to locations outside the EEA without restriction as GDPR does not apply.
- Data transfers to any location are permitted when the data subject or subjects have given unambiguous, free and informed consent for the transfer to take place[32].

## Further information

Information Commissioner's Office

https://ico.org.uk/for-organisations/guide-to-data-protection/

https://ico.org.uk/media/for-organisations/documents/1529/assessing_adequacy_international_data_transfers.pdf

European Union Commission website pages dealing with international data transfers
https://ec.europa.eu/info/law/law-topic/data-protection_en

[31] For a current list of other countries considered to have an adequate level of protection see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[32] This is a defined "derogation" listed in Article 26(1) of the European Parliament and Council Data Protection Directive http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

# *Section 8: Data processing by third parties*

## *Background*

The need to maintain high standards of information processing and handling is not limited to employees of the University of Sheffield. The same duty of care must apply to any person undertaking work on behalf of ScHARR.

## *Policy*

A contract or data processing agreement must be in place detailing how the data will be processed by the third party. Any contract or data processing agreement with a third party must be approved by an authorised signatory in Research Services. Requests should be directed to ri-contracts@sheffield.ac.uk for review and approval (see section 5).

# *Revision history*

***ScHARR Information Governance Policy***

*Version 1 authorised by the Dean, 24/11/2014*

*Version 16-03-31 authorised by the ScHARR Information Governance Committee 31/03/2016*

*Version 17-03-31 authorised by the ScHARR Information Governance Committee 31/03/2017*

*Version 18-03-31 authorised by the ScHARR Information Governance Committee 31/03/2018*

*Version 19-03-31 authorised by the ScHARR Information Governance Committee 25/03/2019*

*Version 19-08-09 authorised by the ScHARR Information Governance Committee 09/08/2019*

*Version 20-04-30 authorised by the ScHARR Information Governance Committee 30/04/2020*

*Version 20-10-13 (this version) authorised by the ScHARR Information Governance Committee 13/10/2020*

| Date | Section | Summary of changes |
|---|---|---|
| 25th March 2019 | General | Minor updates added throughout the policy where more clarity was required. |
| | Overview | Added references to relevant university policies in overview regarding anonymisation, ethics and data management planning |
| | | Risk-bearing data definition updated so as not to imply the inclusion of all unpublished research |
| | Section 1 | Training section updated: ScHARR IG training is annual, Cyber Essentials Assured Computing training is mandatory for anyone who will have access to NHS digital data |
| | Section 3 | Extra information regarding the impact of using Google Drive rather than University network storage on existing procedures added. |
| | | Extra subsections on NHS digital data projects and Data Sharing Agreements added |
| | | Further considerations around using storage on local hard drives / solid state drives and portable devices added |
| | | All audio recordings should only be on encrypted devices. |
| | Section 5 | Extra information and links to University guidance on anonymisation added. Updated DSA templates added. Emphasis added to the signing of DSAs by an authorised signatory in Research Services |
| | Section 6 | Updated to reference the latest guidance on reporting an incident. Also, added instruction to staff on reporting outside of normal working hours. |
| | Section 8 | Requirement for data processing agreements to be signed by Research Services added. |
| 9th August 2019 | General | Following a review of how IT support is provided across the Faculty ScHARR IT support is now provided by the Faculty of MDH IT Team. A new ScHARR group for information governance and data security issues has been established, ScHARR DS. Therefore references to ScHARR IT has been changed to either Faculty IT or ScHARR DS accordingly. |
| | Section 2 | A new subsection regarding hardware restrictions has been added. |
| | Section 3 | Further clarification regarding the restriction of Google Drive added. Clarified the definition and use of audio recorders. |
| | Section 5 | A link to Section 251, accessing confidential patient information without consent, has been added. |
| 17th April 2020 | Throughout | CiCs is now IT Services, web links updated |
| | Overview | Definition of risk bearing data updated to clarify that it includes pseudonymised |

| | | |
|---|---|---|
| | Section 1 | University data security training modules to be completed annually and policy enforcement clarified. |
| | Section 2 | The detailed asset register applies to any study using the DSPT as the security assurance.<br>Clarity added around hardware management (previously called restrictions) and device destruction section added. |
| | Section 3 | High Performance Computing added<br>Extra clarification around limitations of google drive added<br>Updated to include any studies using DSPT as the security assurance on the asset register<br>Additional guidance on data destruction added |
| | Section 4 | Link to COVID-19 specific working from home policy added and removal of requirement for line manager written approval; reworded / restructured to clarify. |
| | Section 5 | Information about privacy notices and opt outs added |
| | Section 6 | Additional text has been added to the policy to ensure the IG Lead is aware of data specific requirements and notification details and discusses these with named liaison with ICO. |
| Oct 2020 | Overview | Definition of risk-bearing updated slightly to personal, sensitive or confidential data; rather than and. |
| | Section 3 | audio / video recording section updated to take into account extended remote working. |