# Process for projects using the Data Security and Protection Toolkit (DSPT) as the security assurance

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

The Data Security and Protection Toolkit (DSPT) is an online self-assessment tool that allows an organisation to measure their performance against the National Data Guardian's 10 data security standards. The ScHARR IG Committee assesses our policies and processes against this tool annually in order to provide assurance that ScHARR practise good data security and that personal information is handled correctly.

Anyone that wishes to use ScHARR's NHS DSPT submission as the security assurance for their project (e.g. projects using NHS Digital Data, PHE data, data obtained using CAG / Section 251 approval) must be a staff member within ScHARR and meet the criteria of Information Asset Owner (IAO) for ScHARR NHS DSPT assured projects, typically either :the Principal Investigator (PI) for the project; or, a work-package lead. As such they must comply with the rigorous set of information security standards set out within the ScHARR DSPT assessment.

The IG spot checks procedure will be followed when a member of the ScHARR IG Committee is contacted regarding the potential to use the NHS DSPT as the security assurance.

The IAO using the ScHARR NHS DSPT as the security assurance, must comply with the following actions:

## Notify the ScHARR IG team

Inform the ScHARR IG committee (either the IG manager or section IG lead) about any project that uses the DSPT as the security assurance, ideally prior to beginning the application process (For NHS digital data, this means prior to beginning the NHS digital Data access Request Service (DARS) application process); but certainly before getting a signed off Data Sharing Agreement (DSA). See https://www.sheffield.ac.uk/scharr/research/information-governance/scharr-information-governance-committee

All DSPT assured projects must be included on ScHARR's DSPT as a security assurance asset register. The IG manager or section IG lead will liaise with the project team to collect the necessary information to populate the asset register, as per the IG spot checks procedure.

# Adhere to ScHARR IG Policies and processes

Read and ensure compliance with the ScHARR IG policy
Read and ensure compliance with the ScHARR process regarding Information Asset Owner (IAO) responsibilities

# Do the necessary training

The IAO must ensure that any individual who will access DSPT assured data has a staff contract at ScHARR, is a UoS student, or has an honorary or secondment contract with the University of Sheffield. The IAO must also ensure that  all individuals who will access DSPT data have a valid record of completion for all mandated training modules throughout the period of their access to the data:

- UoS Protecting Information
- UoS Protecting Personal Data
- UoS Protecting Research Data
- UoS Cyber Safety
- UoS Cyber Essentials Assured Computing
- ScHARR Information Governance

These can be found here: https://infosecurity.shef.ac.uk/

# For NHS digital data only: Read the Data Sharing Framework Contract (DSFC) (link here)

All personnel, prior to accessing or using NHS digital data, must be fully aware of, and comply with the terms and conditions set out in the DSFC and the relevant DSA.

Some notable terms are:

- The data recipient must not disseminate the data further unless NHS digital has specifically authorised this.
- The data must only be used in accordance with the express terms of the DSFC and DSA and for only the purpose(s) outlined in the DSA.
- Results / aggregate data derived from the NHS Digital data may only be shared outside of the immediate project team if they comply with the latest version of the HES Analysis Guide's rules on Disclosure Control (see later).

However, it is important that members of ScHARR accessessing data are aware of all terms.

# Ensure the Data Sharing Agreement is signed by Research Services

All Data Sharing Agreements (for any project, not just NHS Digital projects) **must** be signed on behalf of the University by Research Services (email ri-contracts@sheffield.ac.uk).

For NHS Digital projects the University of Sheffield authorised signatory named in the DARS application must be the Director of Research Services (using the central email of ri-contracts@sheffield.ac.uk; currently Deborah Lodge is the signatory). This will ensure that the DSA will be routed correctly through the NHS Digital online approval portal to Research Services for sign off.

Please also send a copy to the ScHARR IG manager or section IG lead notifying them that it is ready for sign off.

All personnel, prior to accessing or using shared data, must be fully aware of, and comply with the terms and conditions set out in the relevant DSA.

See also Section 5 (Information Sharing) of the ScHARR IG policy.

# Set up your privacy notice (if required)

NHS Digital require a privacy notice for all studies, other data providers may also require this depending upon the type of data provided and regulatory approvals; if you are receiving personal data a Data Protection Impact Assessment (DPIA) or equivalent should be conducted (NB the University Research Ethics Committee (UREC) agreed that obtaining ethics approval is evidence of a staff procedure for carrying out a DPIA, however there may be cases where an additional DPIA is required). The interpretation of the legislation by NHS Digital is that they are processing personal data on behalf of the study, and therefore the study should have a privacy notice in order to meet the legal obligation to inform individuals. There is more information regarding the right to be informed on the ICO website. Please contact the IG team for advice on how to set up your privacy notice. It's expected that the majority of the time the privacy notice will be included on a study specific webpage, usually on The University of Sheffield's website. NHS Digital gives one month after signing the agreement for the privacy notice to be compliant, NHS Digital must be informed when this is done.

# Request data storage and computing resources that are compliant

All projects that provide the ScHARR Data Security and Protection Toolkit as the security assurance **must** ensure that users only access this data using IT Services' Assured Computing. Access to data should only be granted to those individuals who *require* access.

By default, data processing for all DSPT projects should be undertaken on a restricted user-access IT Services' virtual machine (VM). If it is not practical to use a VM for some reason, please speak to your section IG lead to discuss why this is the case.

Please also refer to the "Setup and use of Virtual Machines for risk-bearing data" process. Space on the University networked filestore will be allocated along with the VM. Data should be stored here and nowhere else.

Where an IT Services' VM is not practical, data *can* be processed on a Managed Desktop machine or a YoYo machine under the Assured Computing service, but this is *not* the preferred option for DSPT assured projects. If a Managed Desktop or YoYo machine is used for data processing, data must only be stored in a restricted user-access project folder on the shared university networked filestore ("X drive"). Project folders can be requested by emailing ScHARR Data Security at scharr-ds@sheffield.ac.uk.

DSPT assured data must *never* be stored anywhere other than in the University networked filestore allocated to the VM for projects that use a VM, or in the access restricted project folder on the University's Shared Networked Filestore ("X drive" folder) for those projects that do not use a VM.

Google Drive should **never** be used for DSPT assured data, even though this *may* be listed as compliant under the IT Services' Assured Computing service standards.

See also Section 3 (Data Storage and Storage Devices) of the ScHARR IG policy.

# Notify the ScHARR IG team of any changes

Any changes to the data sharing agreement or to the project team who have access to the data must be notified to either the ScHARR IG manager or section IG lead.
Anyone who has access to the data must be compliant with the processes above.

# Destroy data

Destroy datasets when they are no longer needed or when permission to hold them expires (whichever is the sooner); as per the data destruction process.

Under no circumstances shall the Data Recipient retain the Data without an extant DSA and Contract (or New Contract) in place which relates to that Data.

# Ensure contractual compliance when publishing results

Ensure that any agreements regarding publishing and dissemination and terms within contracts, i.e. the Data Sharing Framework Contract (DSFC) for NHS Digital projects are adhered to. This may be, for example, an agreement to suppress small numbers (typically 1 - 7 [inclusive] and all other numbers rounded to nearest 5) in any quantitative reporting, an agreement to acknowledge the data source, or an agreement to confirm with NHS Digital that any “derived data” are sufficiently derived as to be no longer sensitive.

The DSFC states “In any display of the Data, wherever possible, the Data Recipient must cite the copyright of NHS Digital and/or any licensor of NHS Digital as appropriate as follows: "Copyright © (year), the Health and Social Care Information Centre. Re-used with the permission of the Health and Social Care Information Centre [and/or [name of licensor]]. All rights reserved."

# If there is a data security incident, follow the incident policy

If you discover that data security may be at risk, follow the instructions within Section 6 (Incident Management) of the ScHARR IG policy.