Ensuring Data Security when working remotely v2.0

This version (v2.0) approved IG Committee 27.04.2021

Long-term working from home (or elsewhere off-campus) for most staff has been ongoing since March 2020 and measures have been put in place to reduce the risk of a data breach. This document outlines the key requirements and preparations for working remotely. Please read this document alongside the advice on working off-campus issued by IT Services:
Working from home or off campus - Remote Access - IT Services - The University of Sheffield

This document does not cover students working off-campus; advice for students working off campus can be found here:
Studying from home or off campus - Studying from home - IT Services - The University of Sheffield

Information Security Training

The University has created the Cyber Safety training module based on recognised security practices and the types of attack we've seen at the University while working remotely.
It is important to ensure you are vigilant regarding phishing emails, scam phone calls etc.
The Cyber Safety module, along with the other Information Security Training modules, must be kept up to date in accordance with the ScHARR Information Governance policy.

Your computer and other devices

For Information Governance and Data Security reasons, ScHARR would like all staff to use a University of Sheffield-owned computer rather than a personally-owned computer for their ScHARR work wherever possible. If Windows, this should be a machine running the YoYo desktop. Computers running YoYo meet minimum standards for security.

We recognise that a small number of ScHARR staff will have a good reason for using a personally owned computer. MDH IT can grant an exception for ScHARR staff if we are reassured that minimum security standards are met. MDH IT maintains a log of these requests.

IT Services have issued specific guidance regarding these minimum security standards if using your own computer or laptop. It is likely that staff may have temporary University information or files on their computer, either accidently or due to the computer creating temporary files during processing; therefore it is ScHARR policy that all computers or laptops (as well as mobile devices) are encrypted.

ACTION - If you do not currently have a University of Sheffield managed computer at home, there are three options:
1) take home your desktop computer from ScHARR (please email scharr-covid-19@sheffield.ac.uk to make arrangements)
2) be provided with a work laptop from IT Services (please fill in this form)
3) request an exception to use a personally-owned computer for ScHARR work (please fill in this form).

Accessing information and IT services

IT Services has issued specific guidance on how to safely and securely access information: https://www.sheffield.ac.uk/it-services/remote

REMEMBER - you must comply with any project-specific Information Governance requirements; these **may go over and above** the advice provided by IT Services.

When to use VPN

The majority of online services provided by the University are available without VPN (e.g. email, calendar, drive). Managed and YoYo computers should have Direct Access enabled, meaning that VPN access is generally not required.
However, without direct access, a VPN connection is required for:

- direct access to University departmental and personal storage (often referred to as X: and U: drive storage respectively),
- connection to a virtual machine
- connection to a restricted corporate system (e.g. CIES, CIS, SAP)

We do not recommend using UniDrive for routinely working on files on the University filestore. This may result in problems with version control.

ACTION - To set up VPN see https://www.sheffield.ac.uk/it-services/vpn .
To access the X:drive via VPN see https://www.sheffield.ac.uk/it-services/remote/accessing-files

Information Governance

When working remotely it is essential that information governance and security requirements continue to be met. The exact nature of those requirements will vary depending on the work you are doing and the projects you are working on.

Will I breach my data sharing contract or ethics agreement?

Some data sharing contracts and ethics agreements stipulate that data must not be processed off-campus. Check to see if this is the case for your data. Data sharing contracts and ethics agreements must still be adhered to, even when working remotely.

If the ethics agreement does not allow accessing data remotely, consider whether it would be possible to reassure the ethics committee that remote working would be secure. Also check that remote working is not prevented by information given in participant information sheets, consent forms and other documentation associated with the application. Contact the appropriate ethics committee for advice.

ACTION - If the data sharing contract excludes accessing data remotely, advice should be sought before any such work is undertaken. Contact the data provider for advice; many will authorise remote processing of data (e.g. by using VMs). If remote working can not be approved and if access restrictions are in place on campus, approval can be sought to go into work. Email scharr-covid-19@sheffield.ac.uk to request access.

What if my research study uses the NHS Data Security and Protection Toolkit (DSPT) or Cyber Essentials Plus (CE+) as security assurance?

Data storage and processing using the DSPT or CE+ as security assurance (this includes NHS Digital data and Public Health England (PHE) data and, likely, data accessed via CAG/Section 251 approval) must be undertaken within the IT Services Cyber Security Assured Computing framework.

Working within this framework allows us to demonstrate compliance against a range of required data security standards. The Assured Computing framework restricts where data can be stored, and on which types of machine data can be processed.

Although Assured Computing allows data to be stored on Google Drive, the ScHARR IG Policy requires the use of University network storage (i.e. the X: drive, or the drive that maps to the University network storage that is accessible from a Virtual Machine) for DSPT-assured data. Google Drive must not be used to store DSPT-assured data.

ACTION - You must contact the IG Lead, IG Manager or your Section IG Lead before working on DSPT-assured data (e.g. NHS Digital, PHE, CAG/Section 251) remotely. NHS DSPT assurance is only valid if data assets are registered on the ScHARR IG asset register.

Annex A Sensitive Research Data

If working with individual-level research data (even if pseudonymised/de-identified) or other sensitive research data, there are extra considerations that need to be taken into account.

Checklist for working on participant-level or other sensitive research data

1 Do you have a data sharing agreement (DSA) or contract with the data provider?	Yes / No. If yes, answer question 1a
1a Will you still comply with all relevant data sharing contracts if you are working remotely?	Yes / No. Must be yes
2 Is the work covered by ethical approvals?	Yes / No. If yes, answer question 2a
2a Does the ethics agreement and associated documentation allow (or not prohibit) working remotely?	Yes / No. Must be yes
3 Have you used the Data Security and Protection Toolkit (DSPT) or Cyber Essential Plus (CE+) as your security assurance?	Yes / No. If yes, answer questions 3a and 3b
3a Do you comply with the University Cyber Essentials policy:	Yes / No. Must be yes
3b Do you have approval from a ScHARR IG representative	Yes / No. Must be yes

In order to work remotely on sensitive research data, answers 1(a), 2(a), 3(a) and 3(b) must be “yes” where applicable.

Annex B - Information Governance contacts

IG committee membership

Version control

Version	Effective Date	Summary of changes
1.0	13/03/2020	n/a first version
v2.0	27/04/2021	This is an update to the advice for ScHARR staff provided on the 13/03/2020, previous title: “Coronavirus (COVID-19) and ensuring Data Security if working at home or elsewhere off-campus.” Given the extended period of home working the guidance has been updated to a process document and is no longer only applicable to the COVID-19 pandemic. It also reflects improvements in security and access to University infrastructure made over the last 12 months.