Ensuring Data Security when working remotely v3.1

This version (v3.1) approved by the IG Committee 2024-02-26

Regular working from home (or elsewhere off-campus) for most staff has been in place 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, including the advice to:
“Be aware of your connection and surroundings. Make sure to keep your devices out of sight when not in use, lock the screen when you are away from it, and be careful about who else may be looking at your screen.”
“Make sure you are connected to a safe and secure internet connection.”
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

Your computer and other devices

All Division of Population Health staff should use a University of Sheffield-owned computer computer for their work. If Windows, this should be a machine running the YoYo desktop. Computers running YoYo meet minimum standards for security.
All computers or laptops (as well as mobile devices) must be encrypted.

Accessing information and IT services

IT Services has issued specific guidance on how to safely and securely access information:
Working remotely | IT Services | Staff hub (sheffield.ac.uk)

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)

NB: Even with direct access (or access on campus), the VPN may be required for certain services, e.g. RONIN (for the Secure Data Service (SDS))

ACTION - To set up VPN see Virtual Private Network (VPN) | IT Services | Student hub (sheffield.ac.uk) .
To access the X:drive via VPN see Studying from home or off campus | IT Services | Student hub (sheffield.ac.uk)

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 be adhered to.
If the ethics agreement does not allow accessing data remotely, consider whether it is appropriate to request an amendment. 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. If remote working can not be approved, ensure the work is carried out on campus.

If it is acceptable to process data off-campus, ensure this is only from secure locations and using a secure network[1].

What if my research study uses the NHS Data Security and Protection Toolkit (DSPT) as security assurance?

Data storage and processing using the DSPT as security assurance (this includes NHS England data and, likely, data accessed via CAG/Section 251 approval) must be undertaken in accordance with the process for projects using the Data Security and Protection Toolkit (DSPT) as the security assurance.

[1] Using a secured network that requires a security code to access (such as home Wi-Fi and eduroam). Do not use an open, unsecured network such as public Wi-Fi hotspots, for example at coffee shops, airports, libraries and hotels; these are typically open, unsecured wireless networks.

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

The Division of Population Health 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 England, CAG/Section 251) remotely. NHS DSPT assurance is only valid if data assets are registered on the Division of Population Health 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) as your security assurance?	Yes / No. If yes, answer questions 3a
3a Do you comply with the process for projects using the Data Security and Protection Toolkit (DSPT) as the security assurance	Yes / No. Must be yes

In order to work remotely on sensitive research data, answers 1(a), 2(a) and 3(a) 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.
v3.0	30/05/2023	Updated to reflect that hybrid working is now business as usual and Cyber Safety training is embedded in the IS training curriculum. Everyone should now have access to a work computer. NHS digital is now NHS England. Some changes around CE+ are also reflected. Also clarified that VPN may still be required for some services even with direct access.
v3.1	26/02/2024	Clarity and emphasis around using a secure network added. ScHARR updated to Division of Population Health and links updated where appropriate