ScHARR Certified Data Deletion Procedure

This version (v2.1) Approved at IG Committee Meeting 2023-03-30

This process should be read in conjunction with the document "Technical description of what happens when files are deleted" that describes what happens when a file is deleted.

ScHARR process for requesting certified data deletion:

For data held in a project folder on the X drive

Project team:	Contact ScHARR DS to say that there are data on the X drive that need deleting for which a deletion certificate is required. Give ScHARR DS the project details (name of project and name of X drive folder) and indicate whether all contents of the folder or only certain files need deleting.
ScHARR DS:	Where all contents are to be deleted: remove all access to the control folder and request deletion from Storage & Server. Where only partial contents are to be deleted: Create a new control folder in the project shared area.
Project team:	Copy (not move) all files that are to be retained into the new control folder. Delete all contents of the original folder.
ScHARR DS:	Remove all project team access to the original control folder and request deletion from Storage & Server.
ScHARR DS:	Inform IG lead and IG manager that data have been deleted. Provide email trail (e.g. Topdesk job ticket from IT Services confirming deletion) as evidence.
IG lead / IG manager:	Confirm with the project team that no other copies of the data exist (including manipulated or derived data, unless confirmed as derived by the data provider, e.g. NHS England).
IG lead / IG manager:	Complete and sign the certificate of data destruction (see example NHS Digital Certificate of Data Destruction if applicable) and send to project team; include the details of the data to be destroyed, as outlined in the data sharing agreement (DSA).
Project team:	Check the details of the data that are being destroyed is correct and ensure there are no derived or manipulated data stored anywhere else. If correct, sign and send the certificate to the data provider if required.

For data held in a VM filestore where ScHARR-DS have admin rights to the VM

Project team:	Copy files that are to be kept into a new location (typically, an X drive project folder) that has appropriate access permissions (this should not include the original data, and if it includes derived data this must have been confirmed as such by the data provider according to their process). **Anything left in the VM filestore will be deleted.**
Project team:	Shut down VM. Start menu > ⏻ > Shut down
Project team:	Contact ScHARR DS to say that there are data in a VM filestore that need deleting for which a deletion certificate is required. Give ScHARR DS the project details (name of project and name of the VM).
ScHARR DS:	Contact IT Services to delete the VM and VM filestore.
ScHARR DS:	Inform IG lead and IG manager that data have been deleted. Provide email trail (e.g. Topdesk job ticket from IT Services confirming deletion) as evidence.
IG lead / IG manager:	Confirm with the project team that no other copies of the data exist (including manipulated or derived data, unless confirmed as derived by the data provider).
IG lead / IG manager:	Complete and sign the certificate of destruction (see example NHS Digital Certificate of Data Destruction if applicable) and send to the project team; include the details of the data to be destroyed, as outlined in the DSA.
Project team:	Check the details of the data that are being destroyed is correct and ensure there are no derived or manipulated data stored anywhere else. If correct, sign and send the certificate to the data provider if required.

For data held in a VM filestore where ScHARR-DS do not have admin rights to the VM

Project team:	Copy files that are to be kept into a new location (typically, an X drive project folder) that has appropriate access permissions (this should not include the original data, and if it includes derived data this must have been confirmed as such by the data processor according to their process). **Anything left in the VM filestore will be deleted.**

Project team:	Shut down VM. Start menu > ⏻ > Shut down
Project team:	Contact ScHARR DS to say that there are data in a VM filestore that need deleting for which a deletion certificate is required. Give ScHARR DS the project details (name of project and name of the VM).
ScHARR DS:	Contact IT Services to delete the VM and VM filestore.
ScHARR DS:	Inform IG lead and IG manager that data have been deleted. Provide email trail (e.g. Topdesk job ticket from IT Services confirming deletion) as evidence.
IG lead / IG manager:	Confirm with the project team that no other copies of the data exist (including manipulated or derived data, unless confirmed as derived by the data provider).
IG lead / IG manager:	Complete and sign the certificate of data destruction (see example NHS Digital Certificate of Data Destruction if applicable) and send to the project team; include the details of the data to be destroyed, as outlined in the DSA.
Project team:	Check the details of the data that are being destroyed is correct and ensure there are no derived or manipulated data stored anywhere else. If correct, sign and send the certificate to the data provider if required.

For data held in the Secure Data Service

Project team:	Contact the Secure Data Service (SDS) team regarding data destruction
SDS team:	Ensure data destruction is carried out and documented in accordance with the documented process maintained by the SDS team

Version	Effective Date	Summary of changes
1.0	08-May-2020	n/a first version
2.0	24-Jan-2022	Updated to include the DSH. Process to delete X drive data updated to protect the data from recovery
2.1	30-Mar-2023	Updated to be more generic and cover data destruction for providers other than NHS Digital (now NHS England (merger 1st Feb 2023), but a new template hasn't been issued yet). Also Data Safe Haven is now the Secure Data Service. Other minor typographical changes made.