Management of ScHARR resources on Departmental Storage (typically mapped as the “X: drive”)

Approved at IG Committee Meeting 2021-02-18

This document details processes covering “X: drive” folder:

- New requests
- Management
- User-requested archiving and deletion; and,
- Automatic archiving and deletion.

NOTE: If you require evidence of secure deletion of data you should follow the guidance in the ScHARR Certified Data Deletion Process.

Overview

Project leads are responsible for the appropriate management of research data.

University Departmental Storage provides access-controlled, backed-up file storage.

Access to the ScHARR space on Departmental Storage (typically mapped as the “X: drive”) is managed by the ScHARR Data Security team (scharr-ds@sheffield.ac.uk).

Files are stored within a hierarchical folder structure. There are six types of top-level (“parent”) folders. More details about the types of top-level folders and what they should be used for can be found in Appendix A: Types of top-level folder.

Users should be aware that *moving* versus *copying* files and folders within the university filestore has different effects on access permissions to such files/folders; these may not be as expected. See Appendix B: Important information regarding the effects on access permissions of copying versus moving files/folders within the University filestore.

New requests

Process

Requesting a project, workgroup or user folder

To request a new project, workgroup or user folder, a requester (member of ScHARR staff or student (in the case of student folders)) must complete the “Request New X: Folder” form [https://goo.gl/forms/ue3R0mDUmAaC9Ycw1]. This form gathers the following information:

- Type of folder (project, workgroup or user)
- Folder name
- A brief description (for project and workgroup folders)
- For a project folder, the control folders that are required within the top-level folder
- The name and username of the primary administrator, and (if required) auxiliary administrators (see Management)
- An estimate of the length of time the folder will be needed for
- If it’s a research/KE/Service eval project the ScHARR Research Project Database reference number

Requesting another folder-type

Requests are made by email to scharr-ds@sheffield.ac.uk. These requests may require a short meeting with ScHARR DS to determine requirements.

Creating a folder

ScHARR DS collects the information gathered by the request form and then:

- Creates a new support request in TOPdesk in the name of the requester
- Records the TOPdesk job number against the form data
- Sends a confirmation email to the requester, with the job number and a summary of the request; along with a link to the Information Asset Owner (IAO) process informing them of the responsibility of the IAO
- Records the request in the X: Drive Folders log. A unique folder number is automatically assigned
- The request is checked, and errors are either corrected or clarification is obtained from the requester
- The new parent and any control folders are created in the Folder Management system
- The job is updated and an email is sent to the requester asking for the name and username of all users who need access to each control folder (this will be read only or full access). The final folder details are also included to reflect any revisions
- The job status is set to ‘In progress’, and is followed up weekly if necessary
- Access is granted to ScHARR DS at the parent folder level

- When the list of users is received, for each user (“trustee”) access is only granted once all of the following criteria have been met:
    - The request has been authorised by a folder administrator (or Section Director in the case of extenuating circumstance, such as long term sickness)
    - The trustee has a current University of Sheffield computing account
    - The trustee has completed the appropriate Information Security training modules
- Confirmation is sent to the requester
- The folder is marked as ‘Active’ in the log, which allows it to be picked up in the ScHARR Network Folders sheet, which is available to staff

Management

Background

A full list of all active folders with descriptions and responsible administrators is available in the ScHARR Network Folders spreadsheet.

Folder Administrators

All folders must have a designated Primary Administrator, and may have up to three Auxiliary Administrators. The roles are, collectively, known as "Folder Administrators". If there is a conflict in requests from Folder Administrators, the Primary Administrator's instructions will take precedence.

All folder administrators must be contracted ScHARR staff with the exception of student folders, for which the student is the Primary Administrator - their supervisor(s) must be Auxiliary Administrator(s).

If access is needed urgently and a folder administrator will not be available within an acceptable time-frame (e.g. long-term illness), the primary administrator's Section Director may provide equivalent authorisation.

Responsibilities

- **Folder administrators:**
    - **Authorisation:** to authorise changes to folder structure and additions to access in writing (by email).
    - **Management:** to ensure that data is stored in the correct locations, and is only accessible to authorised users. This includes:
        - responding promptly to emails from ScHARR DS or IT Services colleagues regarding the management and administration of folders for which the administrator is responsible.
        - For primary administrators, nominating a new primary administrator should they leave ScHARR or otherwise seek to relinquish the "primary administrator" role.
    - **Closure:** to arrange for the folder to be archived or deleted (see below) when no longer required.
- **ScHARR-DS:**
    - ensure that users have an up-to-date Information Security training record at the time access is granted
- **All users ("Trustees")**:
    - ensure their own Information Security training record is kept up-to-date

Requesting access for users to an existing folder

A folder administrator should send an email to scharr-ds@sheffield.ac.uk containing the following information:

- Information about the person who needs access (the “trustee”)
    - Trustee name
    - Trustee username
- Information about the folder
    - Name of top-level folder
    - If the top-level folder is a project or transcribing folder, which control folder(s) should the new user have access to
- The access permissions the Trustee should be granted:
    - full: read, write (create, update, and move), delete **[this is the default]**
    - read-only

If the email is not sent by a folder administrator, it will still be accepted if the administrator’s explicit authorisation is included in the email chain. However, if there is any doubt, the request is denied and the requester referred to the ScHARR Network Folders list so they can contact the folder administrator (so the administrator can contact ScHARR DS).

Access is only granted when all of the following criteria have been met:

- The request has been authorised by a folder administrator (or an appropriate substitute under certain circumstances)
- The trustee has a current University of Sheffield computing account
- The trustee has completed the appropriate Information Security training modules

All changes to access are logged, with an email listing the changes sent back to the requesting admin as confirmation.

Requesting removal of access to an existing folder

It is preferable for requests to remove a user’s access to be made by a folder administrator, or a section manager. However, any request made by a responsible person or a senior member of staff will be considered. The priority is to ensure that data is kept safe, and access can be restored later if necessary.

All changes to access are logged with an email listing the changes sent back to the requester as confirmation.

Removal of access to an existing folder other than via request

When staff are about to leave ScHARR, a section administrator informs ScHARR-DS via the “staff leavers” process (see Appendix C), ScHARR DS will remove the leaver’s access on the first working day following their leaving date. This will not require the folder administrator's authorisation and they will not automatically be notified. A folder administrator

(who is not a “staff leaver”) may request that the leaver’s access should be retained; this may require the creation of new University of Sheffield computing accounts for the leaver depending on which department they are moving to, or if they are leaving the University of Sheffield.

All changes to access are logged.

Changes to control folder structure

Changes can be made to the control folders within a top-level folder. This includes renaming, adding, removing or merging control folders, or changing the access permissions of a control folder.

Only ScHARR-DS can make these changes, and changes must be requested by a folder administrator.

All changes to access are logged.

Transfer of folders to other departments

Folder administrators may request (by email to scharr-ds@sheffield.ac.uk) that folders be transferred to the control of other departments within the University of Sheffield. Folder administrators must either:

1. confirm in writing that folders do not contain any “risk-bearing data” (as defined by the current ScHARR IG Policy) and that the transfer complies with any and all applicable ethics approvals and/or contractual agreements; or
2. document how the proposed transfer complies with any and all applicable ethics approvals and/or contractual agreements, especially clauses relating to data management, information security or information governance.
3. If there isn’t an suitable folder administrator the matter will be referred to the appropriate IG section lead if one is obvious or, failing that, be referred to the IG committee for further investigation and subsequent approval/rejection.

Routine maintenance

As part of routine maintenance, ScHARR DS will periodically contact folder administrators to check that the access permissions are still appropriate. See the Routine maintenance of ScHARR resources on University Departmental Storage process. A similar process is followed with archives.

User-requested archiving and deletion

Background

Archive folders can be created at the request of a folder administrator. These are typically used to store data following completion of a project. Archive folders have a named administrator, but are only visible to ScHARR-DS and to IT Services. The administrator can request copies of files or subfolders from the archive. The archive itself is read-only.

Process

1. When a user requests that data is archived the following information is gathered:
    a. Confirmation that the data is either risk-bearing or non-risk-bearing
    b. The archiving period in years
    c. Name of a ScHARR staff member who will be responsible for the archive
    d. A description of the data for audit purposes
    e. A record of original location on the X: drive

2. Once ScHARR-DS have processed the request details of the archive will be emailed to the person responsible.
3. At the end of the archiving period a Topdesk job will be raised in the name of the responsible person. They will be emailed and asked to confirm that the data can be deleted or if the archive needs to be extended with a new archiving period.
4. If there is no response after a week a second reminder email will be sent.
5. If the reminder email also fails to get a response after a week a final email will be sent informing the responsible person that unless they respond the archive will be deleted in two weeks time. If a user is possibly unavailable for response the section administrator will be contacted for clarification
6. If the archive can be deleted then ScHARR-DS will delete the folder, update the archive record accordingly and confirm the actions to the user

Automatic archiving and deletion

Background

When a project or workgroup folder reaches the end of its required life (set either at time of creation or updated by the folder administrator for older folders) an email will be sent to the folder administrator asking if the folder can be deleted.

If there is no response after three emails, or if there is no longer an appropriate person to assume the role of administrator, the folder will be moved into the ScHARR X: drive archive area.

Details of the archive, below, will be emailed by ScHARR-DS to the ScHARR staff member responsible (ex-folder administrator).

- Archiving length will be set to one year
- ScHARR staff member responsible for archive
- Description of data (taken from original description)
- Record of original location on X: drive

At the end of the archiving period the person responsible will be contacted and told that the archive will be deleted in one month unless they request otherwise.

When ScHARR DS are notified of a leaver a check against the archive spreadsheet is made. If the leaver is responsible for any archive folders they will be required to nominate a new ScHARR staff member so that responsibility can be transferred. Failure to do so before leaving results in the matter being raised with the IG committee for a decision.

Appendix A: Types of top-level folder

Files are stored within a hierarchical folder structure. There are six types of top-level (“parent”) folder: “project”, “workgroup”, “section”, “student”, “user” and “transcribing” (see below). The majority of time either a workgroup folder (for simple working) or a project folder (for more structured control) will be used.

For “workgroup”, “section”, “student” and “user” folders, authorised user(s) can create files or subfolders within the top-level folder itself - and all files and folders within the directory tree below the top-level folder inherit the access permission rights of the top-level folder.

For “project” and “transcribing” folders, authorised user(s) cannot create files or subfolders within the top-level folder. ScHARR-DS create one or more subfolders with specific permissions within the top-level folder. These second-level folders are called “control” folders, and are given specific access permission rights. See section below that explains how access permissions for subfolders and files are determined.

Types of top-level folder

Projects involving risk-bearing data should use PR-type folders unless there are compelling reasons not to do so but there are six folder types for the top-level folder:

- **Project Folders**
    - Prefixed PR_
    - No access is granted to the top-level folder
    - There are one or more control folders within the top-level folder
    - Control folders are created by ScHARR DS
    - Each control folder has a group of one or more authorised users
    - Authorised users can create subfolders and files within control folders

- **Workgroup Folders**
    - Prefixed WG_
    - Access is granted at the top-level folder level
    - Authorised users can create subfolders and files within the top-level folder

- **Section Folders**
    - Prefixed SECTION_
    - Access is granted at the top-level folder level
    - Authorised users can create subfolders and files within the top-level folder
    - The primary administrator is the Section Manager
    - Modify access is granted for the Section Manager and specific staff (as required)
    - Read access is granted to all staff within the relevant section

- **Student Folders**
    - Prefixed STU_
    - Named with the student's username
    - Access is granted at the top-level folder level
    - The student is always the Primary Administrator, with at least one of their supervisors listed as an Auxiliary Administrator
    - Access is only granted to the student unless the student requests additional users
    - Users can create subfolders and files within the top-level folder

- **User Folders**
    - Subfolders within a top-level folder called 'users'
    - Each subfolder is named with the user's username
    - The individual user can create subfolders and files within their user folder
    - The individual user is the only person with access to their user folder, and they have full access rights to all files and folders within their user folder

- **Transcribing Folders**
    - Prefixed TRANS_
    - Named with the transcriber's name
    - The Primary Administrator is the manager of the ScHARR Transcribing Team
    - The Auxiliary Administrator is the transcriber
    - One control folder is created per transcribing project, with access granted as requested by the ScHARR Transcribing Team - usually this is:
        - The transcriber
        - A member of the ScHARR Transcribing Team
        - One or members of the project, who is responsible for moving audio files and transcriptions between the transcribing folder and the appropriate storage location
    - Control folders are deleted when no longer required

Other folder prefixes (e.g. FIN, TAG, SARG) are structured as either project or workgroup folder types, but are prefixed differently for grouping purposes

Appendix B: Important information regarding the effects on access permissions of copying versus moving files/folders within the University filestore

Access permissions for files and subfolders are modified (or not) differently depending on whether a file/folder is (i) *moved [cut + paste]*; or, (ii) *copied [copy + paste]*.

- **Newly created** files or subfolders inherit the access permissions of the parent/control folder within which they are created.
- Files and folders that are **copied** into a folder inherit the access permissions of the parent folder into which they are copied. This is because the copy is a new file.
- Files and folders that are **moved** into a folder **retain the access permissions that they had before being moved**. *This behaviour is likely to be unexpected by the user, but it prevents users from inadvertently sharing access with an unauthorised person when a file is moved accidentally.*

Appendix C: Staff Leaver Process

When a member of staff leaves ScHARR, the Section Manager notifies ScHARR-DS by email. A report is sent to the leaver which includes:

- instruction to transfer ownership of any files stored in Google Drive to an appropriate colleague
- instruction to return all allocated hardware to the Faculty IT hub
- a list of network groups of which the leaver is a trustee, and notification that their access will be removed
- a list of network folders of which the leaver is a trustee, and notification that their access will be removed unless a request is received from a folder administrator to retain the leaver's access
- a list of network folders of which the leaver is the primary folder administrator, with a request to nominate a new primary administrator
- a list of network folders of which the leaver is an auxiliary folder administrator, and notification that they will not retain this role
- a list of archives of which the leaver is the administrator, with a request to nominate a new administrator
- if the leaver has a Qualtrics account, notification that the account will be disabled, with instruction to transfer ownership of any Qualtrics data to an appropriate colleague

All access is removed on the first working day following the leaving date, unless alternative instructions are received from an appropriate authority.