Staffordshire University Research Data Management Policy

Preamble:

Good research data management enables the University and its researchers to meet the standards and responsibilities set out in the University's Code of Conduct for Research and Research Integrity (https://www.staffs.ac.uk/research/docs/pdf/research-code-of-conduct.pdf) and to meet funder, ethical, legal and other responsibilities. This policy is binding on all University members engaged in research, including staff, research students, and affiliates, and others who conduct research on behalf of the University. The policy is guided by and adheres to the UK General Data Protection Regulations (GDPR) and the Data Protection Act (2018).

Policy

1. Staffordshire University recognises the importance of establishing appropriate systems, policies and processes to govern the ways in which research data generated as part of the University's research activity are managed.
2. This policy applies to all those undertaking research (including staff and postgraduate researchers) and those managing and supporting research; and to all research, whether externally funded or not.
3. This policy requires that all those undertaking research store unpublished University research data within Microsoft SharePoint through a Microsoft Teams Team[1].
4. It is the responsibility of the principal investigator of the research study to ensure the data for their studies is stored according to this policy.
   It is assumed that research data obtained will be digital, or can be digitised and then stored according to this policy. It is expected that only in very rare cases will it be impossible to digitise the data, in which case the principal investigator should make this clear on the Ethics application, and furthermore make clear how the data will be stored.
   The principal investigator should further ensure that personal data is stored as required by the University's Code of Conduct for Research and Research Integrity, and Annex 1 to that code, the 'Framework for Good Research Practice'[2]; furthermore, a separate Teams channel, or private channel, should be used for personal data. Personalised data and anonymised data should be stored in separate locations.
   The principal investigator is the named lead researcher at Staffordshire University responsible for delivery of the research, or the component of research assigned to the University.
   The principal investigator must describe in the study protocol (or within the research methodology) the name of the Microsoft Teams Team that will be used to store the data, who will have access to the data and what Microsoft Team authority they will have (member or owner).

[1] Data shared within Microsoft Teams is stored in SharePoint.
[2] Code of Conduct for Research and Research Integrity available at :
https://iris.staffs.ac.uk/Utilities/Uploads/Handler/Uploader.ashx?area=composer&filename=research-code-of-conduct.pdf&fileguid=d2008685-3e39-4954-9216-15e6c21236d6
Annex 1 Framework for Good Research Practice available at:
https://iris.staffs.ac.uk/Utilities/Uploads/Handler/Uploader.ashx?area=composer&filename=framework-for-good-research-practice.pdf&fileguid=65b48305-e658-417e-b8ce-20524d369182

Where named individuals are known, this should be given. In roles that are not yet occupied, the role title should be used. It is the responsibility of all researchers who have access to the data to comply with this policy for all research data that they process.
If the 'raw' data is not immediately stored on Teams but is captured on a separate device, the data should be uploaded to Teams as soon as is practicable, which must be within two weeks. If it is known before the research starts that this time scale will not be met, this should be made clear on the Ethics application. Before data is transferred, it is the responsibility of the individual to ensure that it is secured according to the legal standards to which this policy adheres and to Staffordshire University IT regulations (https://www.staffs.ac.uk/legal/it-regulations).
In the case of postgraduate research students, it is the responsibility of both the student and their supervisor to ensure that their research data is stored in accordance with this policy.

5. If the principal investigator leaves the University, they must inform their line manager and their School's Associate Dean for Research and Innovation of the name, description and location of the data.
   If the research study is still ongoing, a new principal investigator will be assigned, and they will assume responsibility for the research data.
   In the event that the research study has concluded, or that no one else remains employed at the University, the Associate Dean for Research and Innovation of the School in which the original principal investigator worked will assume responsibility until the data has exceeded its retention period.
6. In the event that Staffordshire University is not the lead research organisation, it is recognised that data may need to be transferred and/or stored according to other University's policy and procedure.
   Where another organisation's policy and procedure is put in place, the Staffordshire University (via the principal investigator and copying in dataprotection@staffs.ac.uk) should be notified in writing.
7. It is acknowledged that some research data may not be transferred to the University in order to be compliant with legislation. Where this is the case, it should be clearly stated in the study protocol, or within the research methodology before any research activity commences and should be clearly stated in any ethics application documentation.
8. When creating a 'Team' to store research, a separate site should be created for each research project. This enables appropriate levels of access and control to be applied to each project, and simplifies compliance with any legal, contractual or regulatory requirements.
9. When creating a Teams site:
   The site must be given a meaningful name and include the reference number from the ethics application. If the title contains the word "Research" then a default data retention policy is applied to the team site to preserve all files stored on the "File" tab for 3 years.
   Privacy levels must be set to "*Private – only team owners can add members*". This restricts access to just the individuals that have been authorised by the owner of the site.
   Site owners should undertake at appropriate intervals reviews of who has access to the site, and remove access from individuals or add access to individuals as appropriate.
10. To allow researchers to retain data for a specified period of time, Staffordshire University has implemented a policy that detects key words within SharePoint sites' description and applies corresponding data protection policies.

If the keywords “Hold1”, “Hold2”, … , “Hold10” are added to a SharePoint site’s description then data on the site is retained for the corresponding number of years (i.e. 1, 2,…10 years) after it was last modified.

If a greater retention period is required, then Digital Services should be contacted to add a custom retention hold to the site.

11. Similarly, it may be required to delete data after a specified period. The keywords “Delete1”, “Delete2”, …., “Delete10” can be added to a site to delete data a specified number of years after it was last modified.
12. Holds and deletes are calculated for each individual file based on its last modification date.
13. If both “Hold” and “Delete” policies apply to a site, then both processes will take effect. If the retention hold is greater than the delete then files will not be deleted until after the hold period.
14. Note that if required, a researcher can check what hold/delete policies are applicable to their sites by using SharePoint search functionality at https://staffsuniversity.sharepoint.com/_layouts/15/sharepoint.aspx. Searching for e.g. “description:hold5” would list sites with a five year retention period.
15. Researchers who are intending to collect and store highly sensitive/confidential research data should discuss with Digital Services how such data can be protected.
16. This could include:

    Requiring Multi-factor authentication in order to access a team site. This protects from phished/stolen credentials being used to access a site

    Requiring use of a University managed computer to access a team site. This protects phished/stolen credentials being used to access a site, and makes it more difficult to extract data from a site.

    Preventing file download from non-university managed computers, but providing a web edit view to authorised users to allow controlled viewing and editing of files. This make it more difficult to extract data from a site, or for ransomware/malware to be introduced into a site.