quantity of data included where known. If the data volume is likely to exceed 100 GB, this should be stated.

If any of the data outputs will not be suitable for archiving, these should be identified and the reason they are not suitable for archiving stated.

Archiving

Researchers should where possible use UKRI-funded or other data type-specific repositories to preserve and enable access to data. UKRI data repositories include the NERC data centres ReShare repository, and the Archaeology Data Service, funded by AHRC and NERC. BBSRC contributes to a number of international bioscience data sharing resources, including the molecular biology databases of the European Bioinformatics Institute. The Wellcome Trust also maintains a useful list of approved data repositories

partner. If IP protection may be sought, it should be possible to release data once protection has been confirmed.

Further guidance

Storage and computing requirements

Data collected/held at the University should be stored using University-managed infrastructure, which will provide data security, replication in separate data centres, automated backup and file recovery. For the different options available, and information about costs, please read the guidance here.

Data collected in the field should be stored securely and backed up using local devices and transferred at the earliest opportunity to the primary storage location.

Sensitive/confidential data can also be stored in these locations; if such data are stored or shared using other devices or cloud services, this should be in accordance with the University Data Protection, Remote Working and Encryption Policies accessible here.

If you have computing-intensive requirements, custom specifications of CPU, memory, storage and GPU can be purchased from the University on a pro rata basis. Information is available in the Academic Computing Team website.

Storage costs should be based on the volume of data to be generated/collected in the project, and should be identified on the application as a Directly Incurred cost.

Research ethics and data protection

You have an ethical obligation to protect the confidentiality of personal information provided to you by research participants, and you must also comply with data protection law if you collect and process personal data. Where personal data are processed in jurisdictions outside the European Economic Area, they should be handled to the standards prescribed by UK data protection law.

Committee. Guidance can be found here.

Your application for ethical approval and information sheet/consent form should not make any commitment to destroy confidential data by a given time or not to share (anonymised) data collected from research participants. In most cases data can be shared openly if they are anonymised. It is good practice to secure consent for data sharing when you recruit participants, e.g. by including in your consent form a statement

made available in anonymised form, so that they can be consulted and re-used by

The UK Data Service provides excellent guidance on consent and anonymization, and has sample information sheets and consent forms.

If you will be processing personal data in your research, you are advised to consult University guidance on Data Protection and Research. The Data Protection Checklist for researchers is a good starting point. There are also sample information sheets and consent forms.

Personal data is any information relating to an identified or identifiable natural person. These data enjoy statutory protection under the General Data Protection Regulation 2016 and the Data Protection Act 2018. Under this legislation any personal data collected by you must be processed fairly and lawfully. Among other things you will be required to issue a Privacy Notice to your research participants, which explains the purpose(s) for which the data are being collected, your lawful basis for processing the data, who the data will be disclosed to, and the rights of the individuals in respect of their personal data. For certain kinds of research, for example involving the processing of sensitive data or human genetic data, you will need to complete a Data Protection Impact Assessment under the advice of the University Information Management & Policy Services Officer.

You must ensure that personal data are kept secure and are not disclosed to