Ethical Guidelines on Data Storage and Security

(Note that these guidelines have been designed to prevent the *unintended* sharing of data - please see the document titled 'Guidelines for Researchers on Issues around Open Access Data' if you are interested in issues around the *intentional* sharing of data).

The increase in mobile working, cloud-based storage, and unsecured wireless networks have increased the likelihood that data and information can fall into the wrong hands - i.e., be shared *unintentionally.* Ensuring that this does not occur is one of the responsibilities associated with conducting ethical research.

The University provide online training on the basics of research data and security (please visit https://infosecurity.shef.ac.uk). **The training on 'Protecting information' and 'Protecting personal data' are compulsory for all staff and PGR students. The training on 'Protecting research data' is compulsory for anyone working with research data**. There is also a specific module for members of the Department of Psychology describing the departmental procedures for storing work securely and where to go for support and also a module on protecting research data.

Information about the University's information security policies can be found here https://www.sheffield.ac.uk/cics/infosec and CICS may be able to advise on a case-by-case basis where additional guidance is required (contact the CiCS Helpdesk in the first instance helpdesk@sheffield.ac.uk Tel: 0114 222 1111). Note that the UK Research Councils and many charity funders also have policies on the management of research data which apply to their funded researchers. For additional information, see https://www.sheffield.ac.uk/library/rdm There is also specific guidance and help for researchers working in the Department of Psychology here: https://www.sheffield.ac.uk/psychology/research/groups/dmsppsych

One important security issue concerns the **use of public wi-fi**. Connecting your computer or mobile device to public wi-fi is more secure than using a public computer but there is still a risk that your password and/or confidential information that you access could be intercepted. The University therefore suggest that you should use the University's VPN service to protect your communications that if you connect to public wi-fi www.sheffield.ac.uk/cics/vpn If working in a public place please also consider who might be looking over your shoulder etc.

Another important issue is **who is responsible for what students / researchers do with respect to storing and accessing data?** The answer is that the lead applicant on the relevant ethics application is responsible for making the expectations for data storage and security clear (unless this is a student, in which case it is the relevant member of staff). However, it is the student / researchers' responsibility to take heed of this advice and to take the necessary precautions to ensure that their data is secure. As above, we strongly recommend that all members of the research team complete online training on the basics of research data and security (https://infosecurity.shef.ac.uk)

DESC suggest that you also consider the issues around sharing data within the team. For example, who will have access to the data and when? If you have any concerns, then it may be worth having an agreement in place (to which all parties sign up) at the start of the project.

Finally, it is worth considering (in advance) how you will **dispose of (confidential) data.** If you need to dispose of data, or move data from one place to another (e.g., if moving offices), then this also needs to be done so securely. Please consult the University's guidance on how to deal with confidential waste: https://www.sheffield.ac.uk/hs/environment/confidentialwaste

In summary, DESC require that researchers consider the issues around data storage and security **before** collecting any data (e.g., at the point of preparing an ethics application). We recommend that researchers complete the University's online training and prepare a data management plan (e.g., using the tools here https://www.sheffield.ac.uk/psychology/research/groups/dmsppsych/) that can be included alongside the ethics application.

Thomas Webb and Chris Willis, August 2017