



FOSTER

Facilitate Open Science Training for European Research

Scottish Graduate School of Social Science Workshop:
Overcoming obstacles to sharing data about human subjects

Edinburgh, 10 June, 2015

Robin Rice
EDINA and Data Library
University of Edinburgh



Storing sensitive data

- 🌸 Anonymise data before storing.
- 🌸 Store data on institutional which is secure, resilient and regularly backed up.
- 🌸 Password protect data if not on secure server.
- 🌸 Give access to data to only authorised people.
- 🌸 Encrypt data (especially on portable devices).
- 🌸 The University has got a policy for Information Security:
<http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations/security-policies/security-policy>



Encryption

- 🌸 Encryption is the process of converting data into an unreadable code. You must have access to a password or a secret encryption key to be able to read an encrypted file.
- 🌸 Encryption comes in strengths. A higher key sizes takes exponentially longer to crack. A key size of 8 takes 0 milliseconds to crack. A key size of 128 takes 150 trillion years to crack.
- 🌸 BitLocker (Windows) and FileVault (Mac) are currently the University of Edinburgh's recommended software solution for encrypting data:
<http://edin.ac/1GmckMv>

Activity: discussion of a scenario

- 🌻 A researcher encrypts her data folder, then forgets his password and can no longer access his data.
- 🌻 What could she have done to avoid this?

Activity: discussion of a scenario

-  The researcher could have kept a copy of the password but in a separate location to the data folder.
-  Ellie Bates explains how she dealt with this during her postgraduate research study:
(from Research Data MANTRA):
<http://edin.ac/1Gx8xBS>

Migrating /transferring sensitive data

- 🌸 Are you authorised to transfer data?
- 🌸 Is the person who is receiving the data authorised to have it?
- 🌸 Are you transferring the data securely?
 - Use secure channels e.g. SFTP
 - Never use cloud services e.g. Dropbox, OneDrive
 - Never send sensitive data over email unless encrypted
- 🌸 Your university may have a policy on taking sensitive information and personal data outside the secure computing environment: UoE - <http://www.ed.ac.uk/schools-departments/records-management-section/data-protection/guidance-policies/encrypting-sensitive-data>



Disposal of sensitive data

- 🌸 Consider appropriate ways to destroy sensitive data when done with the data.
- 🌸 Shred or secure erase data:
 - Hard drives: use software for secure erasing such as BC Wipe, Wipe File, DeleteOnClick, Eraser for Windows; 'secure empty trash' for Mac.
 - USB Drives: physical destruction is the only way
 - Paper and CDs/optical Discs: shredding
- 🌸 The University of Edinburgh has a comprehensive guide to the disposal of confidential and/or sensitive waste held on paper, CDs, DVDs, tapes, discs and other holding devices: <http://edin.ac/1OtmCo8>

Activity: discussion of a scenario

- 🌸 Digital audio files are emailed to a transcriber who saves them to his computer desktop and also stores them in his email once received. The transcriber fails to delete the files from his email and from his computer once the transcription is completed and returned to the researchers. He later sells his computer on eBay.
- 🌸 What should the researcher have done to prevent this happening?

Activity: discussion of a scenario

-  You should ask transcribers to sign an agreement to destroy their copies of the data once they have been returned and verify after transcription that this has indeed been done. It is best not to email files that you do not want to linger on other people's computer systems. You could encrypt the files before emailing them or send them via secure transmission.
-  Records Management: Confidentiality agreement:
<http://edin.ac/1buAug1>