Protecting Electronically Stored Personally Identifiable Research Data
Quick Reference for Dalhousie Researchers
Prepared by Dalhousie Research Ethics and Information Technology Services (ITS), June 2017

Research participants trust researchers to manage their personal data in a way that is secure and ensures privacy, especially for personally identifiable information. The TCPS2 (Tri-Council Policy Statement 2014) states that “information is identifiable if it may reasonably be expected to identify an individual, when used alone or combined with other available information.” It is the ethical responsibility of researchers to take appropriate steps to protect these data. The Dalhousie Research Ethics Boards in consultation with Dalhousie ITS have prepared this brief document to help researchers plan their research projects in ways that ensure participants’ data are kept securely.

General guidelines:

1) Decide where to keep different types of participant research information
It is important to keep personally identifiable participant information, or codes that link participants to their data, separate from the actual data. The main reason is that if one device/drive (e.g. a laptop) is accessed, participants cannot be re-identified by simply matching up the two documents. It is preferable devices be physically stored separately as well. When deciding where to store codes and/or participant data, researchers should know about the tools Dal offers, along with some important considerations about which to use:

- **NAS drive (formerly Novell)** – NAS is available to faculty, and to students with permission by their department, and is recommended for storing sensitive research data, including any personally identifiable data. Files and folders can be granted restricted access. Data from NAS is stored on secure Dalhousie servers, and can be accessed when connected to the Dal network, or off-campus anywhere in the world through Dal’s VPN (virtual private network – see https://wireless.dal.ca/vpnsoftware.php for more information).
- **One Drive** – One Drive currently stores data on servers outside of Canada; no personally identifiable research data should be stored here (to comply with provincial legislation). Do not store participant code keys on One Drive. Only de-identified or aggregate research data should be stored here.
- **Personal Computer or Laptop** – If storing research data on a computer, the documents should be encrypted and the computer must be password protected. It would be even better to encrypt the computer. Set a time out to automatically lock after a set number of minutes.

2) Prevent data theft/loss
Theft or loss of data is possible. It is your responsibility to take precautions to prevent this from happening, and that means being smart with where your data is stored and how accessible it can be by an outside party. Here are a few good practices:

- **Encrypt your laptop** – FileVault is a tool available for Macs. BitLocker is available for Windows.
- **Encrypt external hard drives** - Always encrypt external hard drives that store research data.
- **Store on NAS** – This is only accessible with a Dalhousie NetID and password. If you are off-campus, you must connect through a VPN (see point above in section 1).
- **Don’t use USB keys** – USB keys are small and easy to lose or have stolen. They are also generally not very stable in the long term. USB keys should be used as a last option, and they should always be encrypted.
- **Password protect computer, laptop, and phone** – Always password protect laptops and computers that store research data. Set a time-out as well so it automatically locks after 5 minutes.
- **Watch your device** – Laptops, USB keys, mobile devices, etc. should be stored safely – lock them in a drawer when not using them.
3) Transfer data properly
Sharing and sending data with other members of the research team can introduce risks. The general rule of thumb is not to transfer via the cloud, and always use secure transfer methods for sending and receiving data. Here are some good options for sharing and transferring data:

- **Use FileExchange** – FileExchange encrypts each file and it’s the best way to transfer any personally identifiable participant data to another person on the research team. Users must add passwords and can expire access to files if needed. FileExchange is designed for transferring files, not long-term storage. Set up an account at [https://fileexchange.dal.ca/](https://fileexchange.dal.ca/).

- **Use Dalhousie/institutional emails only** – but do not email personally identifiable participant information (use FileExchange). If it’s necessary to transfer files to another member of the research team by email, ensure the files only contain de-identified data and are encrypted and send them from Dal email addresses. Make sure all team members receive files directly through their institutional email (and not through a third party, like Gmail, which you should never use for University work).

- **If transferring from mobile device to computer (i.e. audio interview data), use a cable** – do not email files or transfer via the Internet (cloud), and don’t use syncing to transfer files from one device to another.

4) What not to use
Not all tools are suitable for storing participant research data due to storage and security risks. Do not store any personally identifying participant data on:

- Google Docs, Dropbox, Evernote, Box, or other cloud based storage services
- One Drive (for reasons mentioned under #1 above).

5) Some good tools and tips
There are many good tools out there to help you conduct your research. These are just a few of them:

- **Voice memo for iPhone** – This is good for recording interviews. It is easy to prevent auto-syncing to i-cloud and you can keep the data on your phone.

- **Dragon Dictation** – This is a good tool for transcribing interviews.

- **Skype for Business** – This is available through Microsoft 365 and is available to students, staff, and faculty. It is encrypted between each computer so conversations, in text or video, and file transfers are secure.

6) Make a plan that works

- **Be practical!** - Develop a plan that takes into account the security and safety of participant data, but also one that is practical and makes sense for the research team. Start by thinking what you’d like to do, and make sure each step in the process follows best electronic data security practices. There is more than one way to keep participant data secure!

---

For more information on Information Security at Dalhousie, please visit [https://www.dal.ca/dept/its/security/best-practice.html](https://www.dal.ca/dept/its/security/best-practice.html)

Link to the Personal Information International Disclosure Protection Act: [http://nslegislature.ca/legc/statutes/persinfo.htm](http://nslegislature.ca/legc/statutes/persinfo.htm)

Link to the Dalhousie *Policy for the Protection of Personal Information from Access Outside Canada*:
[https://www.dal.ca/content/dam/dalhousie/pdf/dept/university_secretariat/policy-repository/PreotectionPersonalInfo.pdf](https://www.dal.ca/content/dam/dalhousie/pdf/dept/university_secretariat/policy-repository/PreotectionPersonalInfo.pdf)