

GUIDELINE

GDL-69

Secure Storage of Personal Information Accessed under a Research Agreement

Last updated: August 13, 2025 (v1.0)

Researchers who receive access to restricted materials under the terms of a Research Agreement with SFU Archives are responsible for maintaining the security and confidentiality of all personal information they find in or take from the records. These guidelines provide tips to help researchers meet this requirement.

Physical security

Maintain the physical security of the records and any digital storage devices on which they are kept. Records include images of the originals, notes, data-coding sheets or other forms of recording that contain personal information taken from the records; devices include desktop computers, laptops, tablets, smart phones, USB drives, and portable external hard drives. Where possible, records and devices should be kept in locked cabinets when not in active use; they should always be stored in premises that are securely locked when you are not present.

Strong passwords

Digital storage devices should be secured with a strong password required on start-up as well as exit from sleep or screen saver mode. A strong password consists of 12 or more characters and includes uppercase and lowercase letters, numbers, and symbols.

Secured systems

Do not store individually identifiable information from the requested records on a computer file system that can be accessed by any other users except for yourself and, if necessary, other project members. If the computer is on a network, protect it using a strong password to ensure that no one can access it from the network except authorized project members. Each project member should have an individual and unique strong password. The computer system should be equipped with access logs that can identify who has accessed the data.

Lost, stolen or compromised information

If any of the personal information taken from the records is lost, stolen or compromised (accessed in a manner not compliant with the research agreement), contact the University Archivist as soon as possible at archives@sfu.ca.

More information

SFU Information Security Services' website provides guidance and resources for securing data at <https://www.sfu.ca/information-systems/information-security.html>.