

Student Guidelines for the Information Technology Acceptable Use Policy

Table of Contents

1. Physical Security	2
2. Dos and Don'ts of Data Security	2
-  DOs	2
-  DON'Ts	2
3. Device Encryption	2
- Windows Devices (BitLocker)	3
- Mac Devices (FileVault)	3
4. Password Manager Software	3
- Recommended Password Managers	3

1. Physical Security

- Log Out & Lock Screens: Always lock your computer when stepping away from a computer in a lab or public setting.

2. Dos and Don'ts of Data Security

✓ DOs

✓ **Report Suspicious Activity** – If you notice something unusual (phishing emails, unauthorized access, lost/stolen data), report it to IT immediately. Report phishing emails in Outlook using the Phish Alert Report button.

✓ **Use Secure Networks** –Use EduRoam for wireless connections.

✓ **Be careful when using personal accounts, browser extensions can be transferred from one computer to another without you knowing**

✓ **Submit final work in Canvas as Microsoft Word documents or PDFs** – Students can use whatever product they want to create and edit their work but should submit their final work in Canvas using a Microsoft Word or PDF format.

✗ DON'Ts

✗ **Don't Click Suspicious Links** – Avoid clicking on unknown links or attachments in emails; they could be phishing attempts. Please don't forward these on to IT employees.

✗ **Don't use file sharing software not supported by the college** – Avoid using personal subscriptions to Box, Dropbox, or other file sharing software. Use your college provided Microsoft Office 365 account.

✗ **Don't Download Unapproved Software** – Only use college-approved programs to prevent security risks.

✗ **Don't Ignore Security Updates** – Always install the latest updates for your computer, software, and apps to fix security vulnerabilities.

3. Device Encryption

All laptops should be encrypted and any device not in a locked room/area should be as well. Almost every device contains some type of sensitive information. If a device is stolen or lost it could create security issues (this has already happened as well to several employees). Encryption helps ensure access to the data on the laptop/device is secure but also that

someone couldn't gain access to the computer as "you" and then accessing systems or services they shouldn't.

For Windows devices, you could use BitLocker. For Mac devices, you could use FileVault.

For Windows devices:

- **BitLocker** should be enabled for full disk encryption.
 - You can check this by opening the **Control Panel**, navigating to **System and Security**, and clicking on **BitLocker Drive Encryption**. If it's not enabled, the option will be available to turn it on. Make sure you save the recovery key!

For Mac devices:

- **FileVault** should be turned on for encryption.
 - To do this, go to **System Preferences > Security & Privacy > FileVault**, and turn it on if it's not already.

4. Password Manager Software

Writing your password on a sticky note and sticking it to your monitor is convenient, but very insecure; any person who gains physical access to your computer (or just gets close enough to look) can easily steal sticky note passwords. Writing passwords on a notebook and then physically securing it in locked storage is quite secure, but somewhat inconvenient for access. The most secure option is, of course, memorizing your passwords, but memorizing a dozen sufficiently complex passwords is very inconvenient and simply not possible for many people.

Password manager software provides the best balance of convenience and security. These applications allow you to store hundreds of passwords and easily copy-paste them into web browsers and other applications you use day-to-day. This software will itself need to be secured by a password or a key file (which can be stored on a USB drive), but one password is much easier to keep track of than many.

Password managers are the preferred method for storing passwords. Snow College does not have an officially endorsed password manager, but IT can recommend a number of options, both free and paid:

1. KeePass (personal favorite of IT, free to use, can be secured with a key file on a USB drive instead of a password. Interface is a little dated.) - <https://keepass.info/index.html>
2. LastPass (personal account is free, can upgrade to paid premium account with additional features) <https://www.lastpass.com/>

Student Guidelines for the Information Technology Acceptable Use Policy

3. Bitwarden (paid, but has good features for sharing secure notes, like if you need to share a password. Also has a convenient browser extension)
<https://bitwarden.com/>
4. Dashlane (paid, has similar features to Bitwarden and LastPass)
<https://www.dashlane.com/>
5. 1Password (paid, similar to LastPass, Bitwarden and Dashlane)
<https://1password.com/>