Privacy and Access FAQs

Your HSU information system accounts, information technology resources and computing devices are state-issued, and there are fundamental differences between your privacy in using these resources and your personal computing at home.

CSU-wide Appropriate Use Policy

Section 4.3 of this policy states: "The CSU supports and protects concepts of privacy and protects the confidentiality and integrity of personal information maintained in educational, administrative, or medical records. Information stored in CSU information systems may be subject to privacy laws."

But the policy then goes on to provide a list of circumstances under which your email messages or stored files *may* be viewed by others:

- Warrants, HR investigations, IT security investigations, and subpoenae can result in others inside or outside the University accessing your university email account and/or electronic files without your authorization.
- Under the Public Records Act, members of the public can request access to email or documents of any type, in any medium, that were created in the course of conducting university business; there are very limited circumstances under which you can refuse this request.
- In the event of a possible lawsuit, you and the university may be asked to retain all emails or electronic files in your university accounts and to turn over specific search results to the legal teams involved.

Is my campus email private?

Any contents of your campus email account could be accessed in the above circumstances. The ***best practice*** is to maintain a personal account to use for non work-related communications.

Emails sent from your campus account to an off-campus address are no longer under the control or protection of the campus system. You should be aware that any such email may be forwarded to a third party or retained indefinitely by the recipient and therefore should not be considered private in any way.

Are files stored on state owned equipment private?

Electronic files - whether stored on a university issued office workstation, laptop, tablet, network share, or removable storage device (e.g., thumb drive) - are all subject to the privacy exceptions noted above. There is no privacy distinction between work-related files and personal files when stored on state owned information technology devices.

Also, the files of exiting employees are typically made available to their supervisor when they leave the university.

The ***best practice*** is to not use your campus provided computer or university file storage resources to store personal documents in any media as they could be accessed as part of an investigation, Public Records Act request, or lawsuit.

What about my web browsing at work?

While there isn't active monitoring of user behavior and activity on the web at HSU, many actions are automatically logged as part of routine system operations. Those logs can be reviewed as necessary in support of investigating virus infections and legal or HR investigations. Be aware that California law prohibits some activity on state owned computers, specifically the access or viewing of obscene matter.

The ***best practice*** is to confine your web browsing at work to work-related purposes.

What if I perform work on a personally owned device?

Work related documents produced by campus employees are considered work product and remain the property of the institution irrespective of where they are created or stored. Investigations, Public Records Act request or lawsuits could legally require you to produce these documents even if stored on personally owned devices (e.g., computers, smart phones) or in personal cloud based accounts (e.g., DropBox).

(The above statement is not meant to abrogate in any way that faculty authored instructional materials are considered the intellectual property of the faculty member.)

All employees are responsible for maintaining control over any campus *protected information* in their care (see the Data Classification Standard and Records Retention and Disposition schedule). If your home computer or personal smart phone is shared with anyone else (e.g., partners or children) or is otherwise insecure (perhaps the result of viruses or other malware, even if unintentional), or is stolen you could be liable for release of protected data.

The ***best practice*** is to understand what is and isn't *protected information*, and not access or store *protected information* on your home computer, personal smart phone or personal cloud based accounts.