Securing Sensitive, Critical, and Restricted Data at the School of Social Work

As the value of data increases so does the need for taking extra care and precaution to increase data security, especially for sensitive data and files. Many forms of sensitive data exist, some are protected by legal requirements such as those outlined below:

- **FERPA**: The Family Educational Right and Privacy Act of 1974 protects the privacy of a student's education records and allows the student to determine what information should be confidential, and who should have access to that information.
- **HIPAA**: The Health Insurance Portability and Accountability Act of 1996 ensures the privacy of a patient's medical records.
- **GLBA**: The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, contains privacy provisions requiring the protection of a consumer's financial information.
- **PCI/DSS**: Payment and Credit Card Industry Data Security Standards were developed by major credit card companies to support the prevention of credit card fraud, hacking and various other security issues. Compliance with the PCI Data Security Standard is required to accept major credit cards for business transactions on campus.
- **SSN Protection** - Georgia Law (O.C.G.A 10-1-393.8) forbids "publicly posting" or "publicly displaying" individual's social security numbers (SSNs). It also forbids transferring SSNs over an unsecured connection, as well as using SSNs to access web sites, unless also requiring a PIN or password.

The following minimum requirements are being established at the School of Social Work to enhance security of sensitive, critical, and restricted data of our students, employees, donors, and alumni. Please contact the ITS support team (itshelp@ssw.uga.edu) if you have questions and or need assistance.

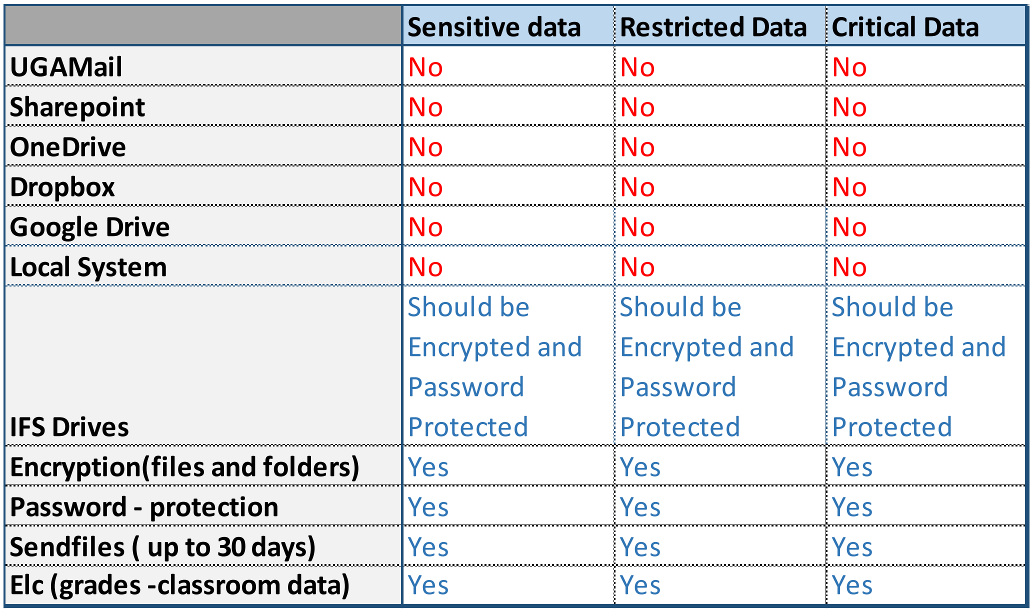
- ***The best place for sensitive UGA data to reside is on its native server or UGA systems.*** If there is no major reason to have sensitive data in one's possession (desktop or laptop or other), leave it on its native server or system, and access it as needed from its native system.
- ***Use UGA's Sendfile / Secure File service (https://sendfiles.uga.edu/) to store sensitive files*** - up to 2GB of storage space with no file expiration. You must log into Sendfile to access any data saved there.
- ***Use UGA's Remote Access VPN to access sensitive data remotely on its native server or system when off campus*** instead of transferring it to a mobile device such as a laptop, or third party hosting services such as Dropbox, Google drive, or Onedrive. For info, see - https://eits.uga.edu/access_and_security/infosec/tools/vpn/#
- ***Store student's grades and classroom data on UGA's eLC system*** - https://uga.view.usg.edu/. If you must store it outside of this system, make sure it is encrypted and or password protected.

Use UGA's Sendfile service – https://sendfile.uga.edu to email sensitive data and notify the recipient that it is on its way so necessary precautions can take place on the receiving end.

Do not use regular UGAmail or Google mail or other personal email accounts to send UGA sensitive data.

UGA sensitive data should not be saved on Dropbox, Google drive, or Onedrive.

The table below summarizes "dos and donts"for storing UGA sensitive, restricted, and critical data.



	Sensitive data	Restricted Data	Critical Data
UGAMail	No	No	No
Sharepoint	No	No	No
OneDrive	No	No	No
Dropbox	No	No	No
Google Drive	No	No	No
Local System	No	No	No
IFS Drives	Should be Encrypted and Password Protected	Should be Encrypted and Password Protected	Should be Encrypted and Password Protected
Encryption(files and folders)	Yes	Yes	Yes
Password - protection	Yes	Yes	Yes
Sendfiles (up to 30 days)	Yes	Yes	Yes
Elc (grades -classroom data)	Yes	Yes	Yes

Suggested Best Practices

If you must transfer or copy sensitive file(s) from its native systems, protect the file(s) by password protecting and encrypting it. It is best to store the file in a secured, university-hosted location such as Sendfiles – sendfile.uga.edu – 30 days only and 2GB file limit.

Store student's grades and other classroom data in UGA's eLC system- https://uga.view.usg.edu/.   If you must store it outside of this system, make sure it is encrypted and or password protected.

Do not store UGA sensitive data on Dropbox, Google drive or Onedrive.

Measures to Protect your Desktop and Mobile Devices and Their Files

Physically lock down desktops, laptops, or other mobile devices such as external hard drives, for example, use locked filing cabinets or storage bins to secure when devices are out of your sight.

Keep UGA mobile devices in your custody or secured at all times and do not pack them in checked airport luggage.

Password protect your desktop and mobile devices with strong passwords or pins you will remember later. Tech support does not keep a log or passwords and cannot be responsible for your password.

Do not post passwords – keep passwords confidential

Change passwords periodically

Encrypt and password protect sensitive files and folders

Do not access sensitive data in public places or access via unsecured wireless networks.

How to password protect files using MS Office applications

1. Click the **File** tab.
2. Click **Info**.
3. Click **Protect Document / Workbook**, and then click **Encrypt with Password**.
4. In the **Encrypt Document** box, type a password, and then click **OK**.
5. In the **Confirm Password** box, type the password again, and then click **OK**

If you lose or forget a password, your file cannot be recovered so use a strong password, but one you can remember.

Passwords are case-sensitive. Make sure that the CAPS LOCK key is turned off when you enter a password for the first time.