SOE FILE STORAGE & BACKUP RECOMMENDATIONS
Technology Department - 2017

ESSENTIAL TAKE-AWAYS

1. SOE Faculty and Staff are responsible for ensuring that their essential data is backed up. There are three mechanisms provided for this:
   a. SOE Servers (T/Common, P/Projects, U/Personal User drives)
   b. Box
   c. Local Backup to external drive (Time Machine, Windows Backup & Restore, etc.)

2. Secure data should not be stored on Box or unencrypted on laptops. (See the Data and Information Classification section.) We are available to consult regarding encryption.

3. SOE Faculty and Staff collaborating using Box should be aware that files belong to only one "Owner." That owner is the person who created the shared folder. If that Owner’s university computing account expires, files in those folders will no longer be accessible. Please consult with us on options for using Box to support essential shared files.

4. Files stored only on local drives (My Documents (PC), Documents (Mac), the Desktop, etc.) may not be recoverable in the event of damage or technical issues on your computer. Files stored on SOE servers or Box should be recoverable.

5. All devices, when left unattended, should be locked with a password or passcode. This helps to protect important data from anyone who gains physical access to your device (a chronic risk in open areas, unlocked offices, coffee shops, etc.).

<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Essential Take-Aways</td>
</tr>
<tr>
<td>Student Guidelines</td>
</tr>
<tr>
<td>Faculty, Staff &amp; Student Employee Guidelines</td>
</tr>
<tr>
<td>Supervisor Guidelines</td>
</tr>
<tr>
<td>Collaborator Guidelines (within SOE or University)</td>
</tr>
<tr>
<td>Projects Guidelines</td>
</tr>
<tr>
<td>Faculty &amp; Staff Guidelines on Use of Box</td>
</tr>
<tr>
<td>SOE Server Drives (U:, T: /Common, and P: / Projects)</td>
</tr>
<tr>
<td>International Travel</td>
</tr>
<tr>
<td>Lost or Stolen Equipment</td>
</tr>
<tr>
<td>Additional Storage and Backup Options</td>
</tr>
<tr>
<td>Other Notes</td>
</tr>
<tr>
<td>Data and Information Classification</td>
</tr>
</tbody>
</table>
STUDENT GUIDELINES

Students should maintain their own backups of all essential files. All students have unlimited space on Box with their university account; any files stored on Box are automatically backed up.

When students receive notice that their Pitt account is going to expire, they should make a copy of files in another location as their access to Box will expire with their Pitt account. Students do not retain access to Box after graduating.

Students with sponsored accounts (who are not enrolled) may need to request access to their Box account.

Any student with an inactive account that re-enrolls within a calendar year will regain access to their files on Box.

Students who are also employees of the School of Education should also refer to the relevant guidelines in this document for Staff.

Faculty, Staff & Student Employee Guidelines

SOE employees are responsible for ensuring that all essential files are backed up. In practice, this means that all SOE employees should be saving files on the SOE servers or Box. Alternatively, files may be saved locally on a machine and backed up onto a second drive (ex. Using Time Machine (Mac) or Windows Backup and Recovery (PC)).

All SOE employees will receive personal space (U: or Home drive) on the SOE servers. They may also receive access to shared folders on the Common (T:) or Projects (P:) drives on the SOE servers. Files saved to these drives are automatically backed up. Retrieval of previous file versions is not a feature on SOE servers. Permissions are administered by SOE Technology Staff and files are recoverable regardless of an employee’s status in the School of Education.

All University of Pittsburgh employees receive unlimited space on their Box accounts. Files saved to Box are automatically backed up and a versioning history is maintained. Access to any files stored in Box is tied to their active status as an employee at the University. Permissions are administered by individual users and files are not necessarily recoverable if an employee’s status changes.

Because of limited recovery options, SOE employees should not use their personal Box accounts for any files that might be essential to operations.

See below for further clarification on the use of Box or the SOE servers.
SUPERVISOR GUIDELINES
As a supervisor, when you become aware of a person’s future departure from the School of Education, before actual termination, you are to ensure that essential files are accessible to appropriate parties.

This may mean that you, as the supervisor, have a copy. It may also mean that a copy of the file(s) is located in a shared folder on the SOE servers. The purpose of this is to ensure that employees do not leave with essential files in their Box accounts, to which we will not have access after their termination.

Another option is to ensure that anyone leaving the University or the School of Education transfers ownership of any relevant files and folders stored on Box before they leave. Otherwise recovering those files or changing ownership may not be possible once the university account terminates.

COLLABORATOR GUIDELINES (WITHIN SOE OR UNIVERSITY)
Anyone collaborating with colleagues or students using Box should be aware that they will lose all access to Box files if the “owner’s” account becomes inactive (leaves the university, doesn’t enroll, isn’t currently on payroll).

Collaborators should make sure to save offline copies of any essential files, or ensure that anyone leaving the University or the School of Education transfers ownership of any relevant files and folders stored on Box before they leave. Otherwise recovering those files or changing ownership may not be possible once the university account terminates.

PROJECTS GUIDELINES
Projects may request space on the SOE Projects server. This is the recommended solution for any Private or Secure data. Users must have Pitt accounts to be able to access.

Projects may request Box storage space for sponsored or resource accounts. This is a possible solution for any non-sensitive data (see http://technology.pitt.edu/mobile-services/box-pitt/box-dtaguidelines.html).

We don’t recommend that projects store any essential files on Box accounts associated with individual users because of the risk of losing access to data if that account terminates. This would affect files, even if they had been shared with users who retain active Box accounts.

FACULTY & STAFF GUIDELINES ON USE OF BOX
Faculty and Staff should not use their personal Box accounts for any files that might be essential to operations. This is because all access to those files may end if the employee leaves the University for any reason.
However, we understand that Box provides useful collaboration tools and that it might be beneficial to use Box when working together on a document or project. As such, we realize that some people may choose to use Box for these purposes. If this is the case, pertinent files also need to be kept on the SOE servers. This is due to the nature of access to Box – once an individual’s account expires, so does their access to Box. This also means that anyone who the expired individual has “shared” with, will also lose access to those files. Therefore, to avoid loss of data, essential files must also be kept on SOE servers.

One possible workflow would be to use Box to develop documents, particularly if input from part-time or non-SOE employees is necessary, but to then save final versions on SOE servers.

Alternatively, Faculty and Staff leaving the University or the School of Education should make sure to transfer ownership of any relevant files and folders stored on Box before they leave. Once the faculty or staff member’s university account terminates, recovering those files or changing ownership may not be possible.

If a faculty or staff member leaves abruptly, it may be necessary to involve General Counsel to apply to get access to files. There is no guarantee that access will be granted, or that it will be granted in a timely fashion.

Files saved on a desktop via the Box Sync client will also disappear if their owner’s account expires.

**SOE Server Drives (U:/Home, T:/Common, and P:/Projects)**

All SOE faculty, staff, and student workers have network storage space available on our own servers, commonly referred to as “the U-drive,” “the T-drive” or “Common,” and “the P-drive” or “Projects.” The drives on the SOE servers are meant for official School of Education files. Personal files should not be kept on these drives. Particularly music and video files are large and occupy large amounts of space that should be used for SOE business.

Our server space is also not designed for projects with large video libraries. If your SOE work necessitates storage of large archives of video, audio or photographs, please consult with the Technology Department before storing collections on the SOE servers.

If they don’t already, the SOE network shares can be mapped to mount conveniently on your computer.

The U: drive belongs to each individual user, and files stored in that location can only be accessed and retrieved by that person. This should be used in place of the local "My Documents"(PC) or “Documents”(Mac) folder.

SOE file servers are accessible to anyone physically connected the network in the School of Education (via a wire to the wall in your office). Off-campus and WIRELESS-PITTNET users will need to authenticate via Pulse Secure before accessing the network shares. No data from the shares resides on the local hard drive, which makes it ideal for Private and Secure data. Do not use Box for Secure data. Do not store Secure data locally on an unencrypted drive, particularly a laptop.

v.2.1
All data on the SOE servers is automatically backed up, however, backups are only retained for 60 days and files stored on SOE servers do not retain versions of files.

- **Home (U:)** Drive – work-related files to which other people do not need access
- **Common (T:)** Drive – administrative work for the School
- **Projects (P:)** Drive – soft-money or short term projects
- **Class (Q:)** Drive – folders related to specific classes

**INTERNATIONAL TRAVEL**

Technology is an essential part of staying connected, including when your work takes you outside the US. There are many information security concerns including loss of the device and hacking of your personal and professional accounts, which may then allow hackers into University systems. The best practice for traveling abroad is not to take your own devices. Fortunately, Pitt has a Technology Loaner Program that provides devices (including laptops, iPads, and smart phones) and limited data plans.

To take advantage of this program is a 3 step process that you should do at least a week in advance of your trip:

1. Register your trip through the [International SOS My Trips portal](http://sos.international.red/)
2. Complete the Technology Loaner Program [Device Request Form](http://globaloperations.pitt.edu/traveling-abroad/technology/)
   (Note: While the service is free, you will need to provide a departmental account number to cover telephone overages or to replace damaged or lost hardware. It’s best to have the department account number on hand before you begin filling out the form.)
3. CSSD will contact you to let you know where and when you can pick up the device(s)

Pitt Global Operations Support provides more comprehensive information both about information security while traveling abroad as well as the Technology Loaner Program (see [http://globaloperations.pitt.edu/traveling-abroad/technology/](http://globaloperations.pitt.edu/traveling-abroad/technology/))

**LOST OR STOLEN EQUIPMENT**

Any SOE owned equipment, or equipment with Private or Secure SOE data on them should be reported as lost or stolen to the Technology Department as soon as they’re noticed missing. We may be able to prevent access to sensitive data if reported in a timely fashion.
ADDITIONAL STORAGE AND BACKUP OPTIONS

In addition to the methods already mentioned, the University also employs SharePoint and OneDrive as options for storage and collaboration.

- SharePoint can be an excellent collaboration tool, and in the SOE, we use it for our Portal. You can also create a personal site with SharePoint, which has many features, and if you use it for document storage/collaboration, it also allows versioning.
- OneDrive is a related tool, similar to Box, and also provides cloud storage for files.

For both SharePoint and OneDrive, the same guidelines apply as with Box: when someone leaves the University, we lose access to their files. Therefore, all essential data should be kept on our servers, and before anyone leaves the University, it should be verified that ownership of files should be transferred. Please see the section regarding Box Guidelines for more detailed information.

If you are considering using OneDrive, this is a helpful chart for you to assess which tool (Box or OneDrive) would best suit your needs. Generally, here in the School of Education, we have a culture of using Box, but you should be aware of the risks & benefits by using either service.

OTHER NOTES

The University of Pittsburgh does not support the use of Dropbox, Google Drive, or other third-party, cloud-based storage solutions.

Files stored only on local drives (My Documents (PC), Documents (Mac), the Desktop, etc.) may not be recoverable in the event of damage or technical issues on your computer. Files stored on SOE servers or Box should be recoverable.
**DATA AND INFORMATION CLASSIFICATION**

<table>
<thead>
<tr>
<th>PUBLIC</th>
<th>Public records are available to the public. Examples include course catalogues, bulletins, press releases, and student directory information. Public data can be stored on the School of Education servers, your computer (desktop or laptop), a mobile device, or on Box. Although confidentiality is not the primary concern, public data may still be essential to operations, therefore, it should always be backed up.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIVATE</td>
<td>Private records don’t contain information in the “Secure” category, but are also not available to the public. Many student records and University business records fall into this category. Private data should primarily reside on the School of Education’s servers. It may also be stored on a desktop computer, laptop, Box, and mobile devices. Private data on these devices should always be protected by a password or encryption. Private data may be essential to operations and, therefore, it should always be backed up.</td>
</tr>
<tr>
<td>SECURE</td>
<td>Secure records contain information that: 1) could be misused by a criminal, 2) the University of Pittsburgh or the School of Education are contractually obligated to keep confidential, or that 3) most people would share only with their family, their doctor, their lawyer, or their accountant. Examples of Secure data include Social Security Numbers, credit card numbers, trade secrets, medical records, tax records, grades for assignments and courses, passport numbers, Veterans Administration data, and bank account numbers. Secure records should be stored on the School of Education servers or according to the higher-level specifications of the respective grant. If absolutely necessary to put secure data on a laptop, the data must be encrypted. Secure data may be essential to operations and, therefore, it should always be backed up.</td>
</tr>
</tbody>
</table>