Best Practices in Securing Sensitive Personal Information

Securing Personal Information of UK Students, Faculty, & Staff

Information Technology Services

Electronic Storage & Disposal

- Do not transmit sensitive personal information via laptop or any other wireless technology.
- Do not transmit sensitive personal information via e-mail or the Internet unless the connection is secure or the information encrypted.
- Do not store sensitive personal information on a laptop computer/desktop computer’s hard drive, USB drive, or other storage media.

Electronic Storage & Disposal (cont.)

- Do not store sensitive personal information in public files accessible via the Internet.
- Do not download sensitive personal information from the University of Kentucky (UK) systems unless legally required.
- Discard media (such as disks, tapes, hard drives) that contain sensitive personal information in a manner that protects the confidentiality of the information.

Physical Storage & Disposal

- Do not take sensitive personal information home.
- Shred sensitive personal information when it is no longer needed.
- Do not discard sensitive personal information in the trash.
- Do not publicly display sensitive personal information or leave sensitive personal information unattended (even on your desk or on the desk of a co-worker).

Security

- Lock your computer when unattended. Using Control, Alt, Delete or engaging a password-protected screensaver are efficient ways to accomplish this.
- Lock offices, desks, and files that contain sensitive personal information when unattended.
- Eliminate the use of forms that ask for sensitive personal information whenever possible.

Security (cont.)

- Password-protect all sensitive personal information and accounts with access to sensitive personal information.
- Do not share passwords and do not document passwords.
- The Gramm-Leach-Bliley act (GLBA), FERPA and HIPAA laws should be followed when dealing with confidential or private information.

Legal Disclosure Requirements

- Do not share sensitive personal information documents or information with anyone unless required by government regulations, specific UK job responsibilities or business requirements.
- Be prepared to say “no” when asked to provide that type of information.
- Do not communicate confidential student information.
- Notify Information Technology Services (ITS) immediately if you suspect sensitive personal information may have been compromised.

Need Help? 218Help@uky.edu

Need to report a security incident? security@uky.edu