Important Information Concerning Photocopier Privacy

We are in an age when protection of confidential, proprietary and personally identifiable information is a risk that must be managed by any organization. Each School and Center at Penn should be aware that, as it administers University privacy policies, it should account for data stored on modern copiers, often viewed as another type of computer that stores data and retains information indefinitely. Just as information is stored on other electronic devices such as personal computers, smart devices and faxes to name a few, copiers and printers also store protected data.

There are over 20,000 copiers, printers and fax machines on campus. End users are responsible to ensure that devices are set up with the appropriate security level. When using these devices, departments should consider the following practices:

1. When leasing a copier, work with your purchasing supplier or leasing agent to ensure that the data processed on a machine has been protected. This is done by encryption or by scrambling the data stored on the machine's hard drive. In some cases data is overwritten or wiped so that reconstructing the data is very difficult.
2. When disposing of or replacing a copier, ensure that arrangements have been made to remove any data stored on the hard drive along with its secure disposition.

To learn more about how you can protect data and ensure that proper controls and security levels are in place, please use your PennKey to log onto ISC's Securing Printers and Multi-Function Devices webpage.