Preparing For School Closure

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

In the event a school needs to shut down, the following best practices and resources can help protect student data.

The Importance of Data Sanitation and Eliminating Residual Data

Educational institutions increasingly collect and maintain large amounts of student data to provide their services. Most of that information, including highly sensitive personal data, may no longer be required by the institution after a student graduates or otherwise leaves school. At this point, it can be destroyed.

Similarly, third parties providing services to an educational institution, such as those conducting research or evaluations, are authorized to receive and use student data. These third parties are also required to destroy student data when it is no longer needed.

This fact sheet offers various methods for disposing of both physical and electronic data to prevent residual data (referred to by NIST as "data remanence") from remaining in memory or storage even after files are deleted using standard methods.

1 Inventory All Hardware, Software, and Accessible Data

- Determine which employees have access to what information. Update permissions and access based on staff changes during the closure period.
- Review all business contracts, checking for obligations and agreements. Ask your legal department for help.
- Track down all "shadow IT" (information technology (IT) systems deployed by departments outside the central IT department), including cloud services — both authorized and unauthorized.
- Check for installed apps to find shadow IT services that employees could access. Delete all relevant data retained by these services.

2 Decommission All Hardware, Software, and Accessible Data

- Designate a core unit for the decommissioning process, and continue to grant them access to networks and assets until the end of the decommissioning process.
- Revoke all other employees' access to networks and other assets immediately after shutting down.
- Reclaim all school devices.
- Delete school data from online services prior to closing accounts.
- Search for any remaining loose threads or existing access points.
- Terminate all remaining accounts and revoke all access.

3 Physically Destroy or Properly Sanitize All Data Storage Devices

Often, when a file is deleted, only the reference to that file is removed, but the data inside the file remains. Specific methods are necessary to permanently delete the data to reduce the risk of that information being recovered by unauthorized users:

- Abide by your school's data destruction policy. All schools should create one.
- Pay attention to compliance requirements when destroying or archiving data and share specifics with the destruction team (e.g., policies may require video of devices being destroyed).
- Shred physical documents and properly dispose of storage devices (remove hard drives, including "HDD" and/or "SDD," from desktops and laptops prior to disposal).
- Identify which data-containing hardware will be repurposed and which will be destroyed. Then, sort all storage devices for purging (overwriting several times), degaussing, and/or physical destruction.
- Be sure to obtain proper certificates of sanitization and documentation to satisfy compliance requirements. For additional information, please review the NIST Guidelines for Media Sanitization.

Data Destruction Best Practices

Consider the following general best practices for data destruction, according to the NIST Minimum Sanitization Recommendations for Media Sanitization:

- Create formal, documented processes for data destruction within your institution and require your partner organizations do the same.
- When drafting written agreements with third parties, include provisions specifying that all personally identifiable information (PII) provided must be destroyed when no longer needed, including copies in system backups, temporary files, or other storage media.
- Specify in writing the type of destruction to be carried out based on the sensitivity of the data.
- Ensure accountability for destruction of PII by using certification forms describing the destruction process and signed by the individual performing the destruction.
- Use appropriate data deletion methods to ensure electronic data cannot be recovered. Talk to your IT professional to ensure these methods are consistent with technology best practices.
- Manage non-electronic documents (letters, reports, invoices, etc.), which may also contain PII, just like electronic data; destroy it when it is no longer necessary so it is safe for disposal or recycling.
- Avoid using file deletion, disk formatting, and "one way" encryption to dispose of sensitive data. These methods leave most of the data intact and vulnerable to retrieval by bad actors.
- Destroy CDs, DVDs, and any magneto-optical disks by pulverizing, cross-cut shredding, or burning.
- Sanitize faulty storage media, either under warranty or service contract, before returning it to the manufacturer for service or replacement. Many data breaches happen this way.

Important Informational Links

- Guide for Conducting Risk Assessments
- Guidelines for Media Sanitization
- Security Categorization of Systems Holding Federal Data