Heller School for Social Policy and Management

Data Destruction Procedure for Secure Data

When secure data is no longer covered by a data use agreement, all copies of those data shall be destroyed. The data destruction procedures to be followed by employees of the Heller School and all research partners are described as follows:

Paper Documents
Destruction procedures for paper documents include shredding the documents using an industry-acceptable shredder, and disposing of the waste in a secure manner.

Electronic media and other media
Destruction procedures for electronic media and other media shall include a triple swipe method for safe deletion of sensitive material. Heller operationalizes this using a program called File Shredder that can be downloaded at the following address: http://www.fileshredder.org/.

If secure data cannot be properly erased from the device, the hard drives or other components containing the personal information shall be securely destroyed by breaking the drive, or the drive or unit must be wiped by a suitable degaussing magnet.

Zip drives, floppy disks, etc. and optical storage media
Prior to disposal, all electronic data storage media such as external hard drives, zip drives, tape drives, floppy disks, memory cards, memory sticks, USB flash drives, or other electronic storage media containing secure data shall have the data contained in the item destroyed by either using File Shredder, by physically destroying the media through shredding or similar physical destruction, or by wiping the media with a degaussing magnet

CDs, DVDs and other optical storage media must be disposed of by physical destruction of the media, such as by shredding.

When data destruction is complete, the employee or research partner must submit a Heller School Certificate of Disposition (COD) to the Principal Investigator. The Principal investigator will notify the originator of the data if required to do so by the data use agreement.