How to Securely Delete Files on a Windows Computer

Welcome to how to securely delete files on a Windows computer. When you routinely delete a file on your Windows computer, it is sent to the recycle bin, and even if you empty or delete what's in the recycle bin, the files remain on your hard drive and can be retrieved by recovery utilities. So for instance, if I delete this file by right clicking on it and choosing delete, the Window asks me, "Are you sure you want to move this file to the Recycle Bin?" If I say yes, the file will now appear in the Recycle Bin. And in this Window I can now empty the Recycle Bin, or I can right-click on it and choose to empty it. The window that appears will say, "Are you sure you want to permanently delete this file?" and I'll choose yes. Although I have chosen to permanently delete the file, it is still on your hard drive and can be recovered by recovery utilities.

However, many utilities exist that will completely erase a file by overwriting it several times. One tool that OET uses on Windows computers is called Eraser. Eraser can be found at eraser.heidi.ie or you can Google it. There's a download button here for you to download and install it. Once it's installed on your Windows computer, you can right click on a file and choose Erase. This will allow a window to appear and it will ask you, "Are you sure you want to erase" whatever the file is. You would click on options at this point, choose Erase with the number

two option and 7 passes and click OK and then you would choose yes. This allows the file to be overwritten seven times to the Department of Defense's standards. This deletion method is secure and can be used for general files.   If you want to securely erase all the files in the Recycle bin or the files that have been deleted from the recycle bin but are still retrievable, right click on the recycle bin and choose Erase Recycle Bin (7-pass DoD). For instance, I am going to move this folder to the recycle bin. I am going to right click on it and choose, erase Recycle Bin, 7-pass DoD. It's going to ask me, "Are you sure you want to erase the contents of the Recycle Bin?" and I'll say yes. The Recycle Bin is now erased and there are no files on it and the files are not retrievable.

If you reassign a computer to another person or are sending it to surplus, OET will securely wipe the computer's hard drive of all data. In this case, you will not need to delete files individually as OET will securely erase all the files from the hard drive.

On a side note, it is a good idea to routinely search for and to delete files that you no longer need or files that contain PNPI, personal non-public information.   If personal, non-public information absolutely must be stored locally in the unit, it

must be encrypted per University policy. However, it is always best to delete any files with PNPI, if possible.

For further information on tools to securely delete files, visit www.oet.udel.edu.

And as always, if you have questions, please contact oet-help@udel.edu.