Managing Personal Storage on your H: Drive
Records Management Quick Tips

These four quick tips will help you clean up your personal (H:) drive and reduce your information storage footprint. Take 5 minutes to try out just one tip – that's enough to make a real difference!

Personal network folders (i.e., your Desktop folder and other locations managed as part of your H: drive on the government network) can serve as a useful short-term workspace or temporary storage for convenience copies, transitory drafts, and other working materials. But they are not appropriate for long-term storage of information. Why not?

- Information is not accessible to your coworkers (who may need it for operational purposes, or to respond to a legal or FOI request).
- Personal drive storage costs are charged to ministries based on volume and are more expensive than most other alternatives.
- If unattended, the accumulation of files will eventually make it difficult for you to find needed information, however convenient the location.

Bottom line, failing to manage storage on your H: drive is costly and puts government information at risk.

Are these files transitory (e.g., convenience copies, working notes)?

Before deleting any files, ask yourself:

- Does this file contain important government information that is not stored elsewhere? If so, move it to EDRMS CM or another secure, shared location such as a LAN drive.
- Do I know what this file is? Do not delete any system files that may be needed for technical purposes (e.g., files in your "Profile", "TRIM Data" or "Offline Records" folders).

For more help, see the Transitory Information Quick Tips RM Guide.

Tip #1. Find and manage files on your H: drive

Cleaning up your H: drive is easier than you think, even if you have many folders and subfolders.

Use the search function in File Explorer (or Finder on Macs) to find files by **type** or **keyword**, regardless of how your drive is organized (or not organized, as the case may be!). The search function is an easy way to find and view files no matter what folders and subfolders they are stored in:

1. Open File Explorer. (Hint: use the search on the task bar at the bottom of your screen to find 'File Explorer'.)
2. Click on your personal (H:) drive. You can identify your H: drive by looking for the network location with your IDIR in its name, like JDOE$.
3. Use the **Search** box to look for
   - **common file types:** e.g., "doc", "docx", "ppt", and image files "jpg", "gif", "png", "tif"
   - **keywords:** e.g., "draft", "version", "superseded" or "v."

4. Under the **View** menu**,** select **Details** to see helpful information about each file in your search results (Name, Date modified, Type, Size, Folder) and enable you to sort them by:
    - **Name**, to locate files with similar names that may be duplicates.
    - **Date modified**, to locate your oldest files. They may be ready to either delete or move.
    - **Size**, to see the largest files. Consider moving them to a more appropriate location or deleting them if transitory.

Tip #2. Remove personal records

Reasonable personal use of government IT resources is permitted under the Appropriate Use Policy. However, storing personal documents (e.g., photos, vacation plan spreadsheets) on your H: drive takes up space and makes it difficult to find your work-related information.

Regularly scan your H: drive for personal files and delete them, after copying any you wish to keep to a personal storage device.

Tip #3. Move sensitive files to a safe location

Sometimes we store sensitive or confidential information on our H: drive because we want to protect it, but we don't have another secure place to put it.

The problem with this approach is that when you are absent or have left your role, these important records are unavailable to your ministry. There's also a risk that you will accidentally share sensitive information.

Here's what to do in Windows:

1. Open your H: drive in File Explorer. Navigate to a folder with sensitive files (e.g., from an HR process or a high-profile policy issue).
2. Find a file that you've been storing there just to keep it secure/private.
3. Save this file in an appropriate location (e.g. LAN drive or EDRMS Content Manager folder with restricted access – see EDRMS Tip 015: Moving Documents from LAN Folders to EDRMS Content Manager).
4. Do you have other sensitive files? Look for more files you can move.

For advice on creating a secure location if you don't have one, see the Appropriate Recordkeeping System RM Guide.

Tip #4. Empty your recycle bin

A little-known fact: items that you delete and move to your recycle bin are still stored on your H: drive and, until these items are emptied from your recycle bin, they are still subject to FOI requests.

It's okay to empty your recycle bin! Emptying your recycle bin (also known as double-deleting) is recommended and is consistent with good government information management practice.

Best practice is to schedule your recycle bin to empty automatically. You can find instructions for how to do this online, including how to empty the Recycle Bin automatically on schedule in Windows 10.

Alternatively, empty your recycle bin regularly. Here's what to do:

1. Right click the Recycle Bin icon on your desktop, and
2. Select "Empty Recycle Bin"
3. Set yourself a monthly reminder.

It's that easy!

Additional Information

Contact your Records Officer and check out the Records Management website.