BRYN MAWR COLLEGE

June 2017

Library & Information Technology Services

Guide to Cleaning your Inbox of Sensitive Data

Please review the following in full before beginning to clean up your inbox. If you have any questions about cleaning up your inbox, contact the Help Desk (help@brynmawr.edu or x7440).

If you haven't already, please review the Top 11 Tips for Cleaning-Up Your Files: http://techdocs.blogs.brynmawr.edu/6416

Why Clean Your Inbox of Sensitive Data?

It's that your inbox is a treasure-trove of sensitive information. Many of us also have our College email synced to mobile devices, which adds additional risk to having any sensitive data lingering in our inboxes. By taking action and deleting unneeded sensitive data and/or relocating data that should be stored in a more secure location, you're significantly reducing the chance that criminals will be able to obtain the data if your account is compromised.

It's important to remember that cleaning your inbox should be a regular practice we all participate in to ensure the security of the College community, as well as our friends and family. While it is important to efficiently organize your inbox, this guide is focused on locating and deleting (or relocating) sensitive data.

What Doesn't Belongs in Your Inbox?

Keeping sensitive data (e.g. credit card numbers, social security numbers, data governed by FERPA, or any personally identifiable information) stored in your inbox increases the risk that it will fall into the wrong hands. In fact, certain types of data are prohibited from being stored in your inbox. Please refer to the College's Data Handling Policy and Data Handling Storage Guidelines. Contact the Help Desk for additional guidance.

The nature of our work sometimes dictates a need to have sensitive data stored in our inbox; however, any sensitive data that is no longer needed or that can be stored somewhere more secure should be removed from your inbox.

Cleaning-Up Your Inbox To-do List

Start off your inbox clean-up with the following actions:

1) Locate sensitive data within your inbox

Think about senders who would be likely to send you sensitive data. Use the Outlook Web App's search and filter tools to locate these messages. Another good place to start might be looking through messages with attachments.

- Check out a quick overview of OWA's search tools here: http://lits.blogs.brynmawr.edu/7031
- Use Advance Query Search to locate messages with specific criteria. See this Tech Doc for more information: http://techdocs.blogs.brynmawr.edu/5670

2) Delete messages from your inbox that contain sensitive information that you no longer need

If the data either is not permitted in your inbox or can be easily retrieved from an alternate source in a secure location (e.g. BiONiC, Financial Edge, Moodle), don't store it in your inbox. If you know you'll need the data in the future and will be unable to retrieve the data from an alternate source, read on to the next to-do list item about relocating sensitive data.

Be aware that even after you delete messages from your inbox, they will remain in your Deleted Items folder for 30 days. After 30 days, those items are automatically moved to the second-stage (Dumpster) for another 30 days. For extra protection, be sure to clear out your Deleted Items folder and the Dumpster. For instructions on how to recover messages you deleted accidentally, see Microsoft's website: https://support.office.com/en-us/article/Recover-deleted-items-or-email-in-Outlook-Web-App-c3d8fc15-eeef-4f1c-81df-e27964b7edd4

Hint: Make quick work of large quantities of unwanted email by creating a **Sweep Rule**. Sweep rules provide various options for deleting or archiving all messages from a particular sender. See Microsoft's website for more on Sweep rules: https://support.office.com/en-us/article/Organize-your-Inbox-with-Archive-Sweep-and-other-tools-in-Outlook-com-or-Outlook-on-the-web-19eee6b9-09a1-4db6-b5d6-37644190884f

Note: LITS recommends that all employees follow existing file retention policies for digital files. See the College's Record Retention Policy here: http://www.brynmawr.edu/humanresources/Internal/Record_Retention_List.pdf

3) Relocate sensitive data from your inbox to the H: or S: drive

Have sensitive data in your inbox that you'll need to use or reference in the future? Consider saving it to the H: or S: drive and deleting it from your inbox. Again, if the data can be easily retrieved from an alternate source in a secure location, don't store it anywhere else.

Note: Again, please remain mindful of the Data Handling Policy and Data Handling Storage Guidelines when considering storing files containing sensitive data on any storage medium. Certain types of data are not permitted to be stored in your inbox, H: drive, or S: drive.

Actions to Take Moving Forward to keep Your Inbox Secure

1) **Does someone send you sensitive data unnecessarily? Ask them to stop!**
2) **Log out of your College email when you're finished**
3) **Protect your mobile devices and computers with a strong pin or passphrase:** See more information on passwords here: http://techdocs.blogs.brynmawr.edu/335
4) **Lock your mobile devices and computers when not in use**
5) **Learn how to recognize phishing attacks and other scams**
    - If you haven't done so, complete the College's Information Security Education Program: http://lits.blogs.brynmawr.edu/7100
    - LITS' Tech Doc SCAMALOT series: http://techdocs.blogs.brynmawr.edu/search-results?q=scamalot
    - Email Spam & Phishing Tech Doc: http://techdocs.blogs.brynmawr.edu/2499