Eastern Mennonite University
Information Security and Technology Code of Responsibility for Employees

My use of the EMU network constitutes agreement to the following:

1. I will abide by all EMU Information Systems (IS) Policies at https://helpdesk.emu.edu/confluence/display/HLZ/Information+Systems+Policy.
2. I will not engage in prohibited activities, including, but not limited to:
   a. Using technology resources to threaten or harass others, even as a joke.
   b. Knowingly distributing malware, phishing emails or other malicious communication.
   c. Attempting to gain access to computers or network accessible resources for which I am not authorized.
   d. Hosting for-profit activities using EMU resources (e.g. selling items for personal profit or promoting a personal business—with the exception of advertisements in the eClassifieds system on www.emu.edu).
   e. Using the EMU network or other technology resources for criminal or malicious activities.
3. My account (Royal username and password) identifies me to EMU systems. I will safeguard my account by:
   a. Not allowing others to use my EMU accounts; nor will I use someone else's account.
   b. Securing my computer against unauthorized access, including using a password-secured screensaver.
   c. Not leaving my computer unattended without securing it by either logging out from it or using a password-protected screen saver.
   d. Using strong passwords[1] and not storing my password(s) in places where others can easily see them.
   e. Treating login pages and requests for my password with skepticism. IS will never ask for your password.
4. I will respect all copyright laws by not infringing others copyrights[2].

   The Digital Millennium Copyright Act (DMCA) provides strict rules governing the use of copyright protected materials. [www.copyright.gov/legislation/dmca.pdf]When EMU receives notification of alleged copyright infringements, the computer owner (if computer is not owned by EMU) or the computer user (if the computer is owned by EMU) will face disciplinary actions outlined in the Responsible Use of Information Technology Resources Policy.
5. I will report any suspicious activity related to electronic equipment or information systems to my supervisor or the IS Help Desk.
6. I will safeguard the integrity and security of personal or confidential information by:
   a. Not knowingly including false, inaccurate or misleading data in records or reports.
   b. Not inappropriately sharing confidential information gained by my position, nor benefiting from it.
   c. Accessing information only to the extent I need it to perform my job responsibilities.
7. I will accept responsibility for ensuring the appropriate use and confidentiality of constituents' information according to the Family Educational Rights and Privacy Act (FERPA) and all other applicable federal, state and local laws and regulations.
8. I will properly secure and/or securely dispose of all documents containing EMU constituents' personal information (e.g. EMU ID numbers, Social Security Numbers, birth dates, addresses, and any other personally identifiable information). I will not store this data in cloud storage systems except EMU's Google system. If I store this data on a personally-owned devices (laptop, tablet, smartphone, etc.) I will secure it with strong passwords, encryption and other measures as appropriate.
9. I will always ensure that my email is stored securely and I agree not to configure my emu.edu email account to automatically forward to any other email address.

Employee's signature _____ Date _____

EMU ID# (if known) _____

Employees may be periodically prompted during the network login process to affirm that by using the EMU network they are agreeing to this code of conduct.

Distribution: Faculty/Staff Handbook

[1] Refer to EMU strong password recommendation at https://helpdesk.emu.edu/confluence/display/HLZ/Royal+Account+Security

[2] Examples of copyright infringement include: Downloading digital formats of music, videos or other electronic media resources and using/sharing them with others without copyright holder permission, using peer-to-peer networks or similar utilities to download copyright protected music, movies or software without permission from the copyright holder, using corporate logos or corporate owned photos without permission