Security Tips for Using MPS Staff Computers

1. **Control access to your machine**
   Do not leave your computer unattended when you are logged on. Leaving your computer unattended while logged in, allows an opportunity for someone else to access your documents, online accounts, etc.

   When stepping away, even if only for a couple minutes, lock your computer/Chromebook:
   - To lock a windows computer, simultaneously press the Windows key and the letter L.
   - To lock a Chromebook, use the Search key and the letter L.

   Students should not use or attempt to fix a teacher's computer under any circumstance.

2. **Choose strong passwords**
   - Strong passwords use a combination of letters, numbers, and special characters to create a mental image or an acronym that is easy for you to remember.
   - A good password is 10 or more characters in length, with a combination of uppercase and lowercase letters, plus numbers and/or symbols, such as pAMPh$3let.
   - Create a different password for each important account, and change passwords regularly.
   - Use a unique password for each account so one compromised password does not put all of your accounts at risk of takeover.
   - **Do not write your password on a piece of paper and tape it to your computer or hide under your keyboard.**
   - **Do not give your password out to anyone especially students**.

3. **Patch, Patch, PATCH! Computer Updates!**
   An unpatched machine is more likely to have software vulnerabilities that can be exploited. Your computer/Chromebook is automatically setup for software and operating system updates. Although it may be an inconvenience, updates are necessary. You will be notified when shutting down your computer that it needs an update. Be prepared that updates may take some time to complete. Please be patient and do not interrupt the process.

4. **Use email and the Internet safely**
   Ignore unsolicited emails, and be wary of attachments, links, and forms in emails that come from people you don't know, or which seem "phishy." Avoid untrustworthy (often free) downloads from freeware or shareware sites.

5. **Protect sensitive data**
   Reduce the risk of identity theft. Store your documents on the H-drive for safe storage and easy access. The district backs-up documents stored on H-drive so they are protected from loss. Securely remove sensitive data files from your computer's hard drive and removable media (Flash Drives, USB sticks, SD cards etc.), which is also recommended when recycling or repurposing your computer. You can sign up for free scam alerts from the FTC at ftc.gov/scams.
   In addition, placing sensitive and confidential data in a cloud environment (Google Drive, Drop Box, and OneDrive) is not secure and not permitted.

   It is important to remember that it is your responsibility to protect student data.