Remote Learning Best Practices for Privacy and Security

The following is a collection of best practices to preserve the privacy and security of student and teacher information:

1) Ensure all computers used for remote learning are up-to-date on security patches and antivirus software, and enable the personal firewall on the computer
2) Use private or home-based networks for remote learning whenever possible. If you must use a public Wi-Fi network for remote learning, do not conduct sensitive personal transactions (e.g. online banking or shopping) over that public Wi-Fi connection, as they can be observed and recorded by anyone else on that public connection
3) Do not download or install any applications on the remote learning device unless explicitly directed to and approved by the school
4) Do not run applications which are not a part of the current learning session and could affect the performance of the remote learning session – such as gaming applications or streaming media (YouTube)
5) Minimize *as much as possible* the entry or use of student or teacher personally identifying information (PII) in any remote learning application. Any "optional" information fields presented by an application should be left blank.
6) Remember that even secure, vetted applications can be misused during a session – if you see student PII being entered or displayed in an inappropriate manner, shut down the session and restart it. Warn all participants about minimizing the use of student PII.
7) Stick to known and previously vetted remote learning applications or online learning portals ("go with what you know")
8) Applications that have been vetted against the NH Minimum Standards by another New Hampshire school district should be acceptable for other schools to use (concept of reciprocity)
9) Applications that can demonstrate national or international security assessment and certification should be acceptable for use by any NH school. Examples of recognized security certification standards which meet or exceed the NH Minimum Standards include: NIST SP 800-171, NIST SP 800-53, ISO/IEC 27001, SOC 2, and FEDRAMP.
10) Know who to call if you see unusual or suspicious internet activity, oddly behaving applications or a cybersecurity incident on your remote learning device