NEN – The Education Network

e-Security: 10 steps to protect your school's network

November 2014

This document is intended for school senior leadership teams and provides an overview of what needs to be in place to keep school networks secure. The 10 steps described here are adapted from the CESG document *10 Steps to Cyber Security*[1]. CESG is the information security arm of Government Communications Headquarters (GCHQ). Make sure you understand where the responsibilities for maintaining all these systems and processes reside: some may be maintained in-house while others may be provided by your broadband supplier or another third party. For more detail about any of these steps, see the accompanying NEN documents *NEN Information Sheet 6: e-Security – Managing and maintaining e-security/cyber-security in schools*[2] and *School e-Security Checklist*[3].

1. Ensure the importance of and responsibilities for maintaining e-security are acknowledged by senior school managers and governors. Make sure your school's Acceptable Use Policy (AUP) for IT is up to date and addresses e-security sufficiently. It is strongly advisable to develop and maintain a specific e-security policy as well.
2. Establish and maintain inventories of all hardware and software used in school that also describe how these are to be configured, reviewed and kept up to date (patched). It is strongly advisable to lock down the configurations of all hardware and software to prevent intentional or accidental misuse.
3. Ensure appropriate technical measures are in place to protect your school's network. These include firewalls, filtering for malicious as well as inappropriate content and antivirus and malware checking.
4. Ensure user privileges (for teaching staff, administrative staff and pupils) are set appropriately so all users can access the facilities they require while minimising the potential for deliberate or accidental misuse of the network. A password policy should be enforced so that strong passwords must be used; these should be changed at regular intervals.
5. Ensure all users, staff and pupils, understand their e-security obligations and responsibilities through appropriate user education and training. The school's IT AUP is a key tool in this regard.
6. Establish and maintain proper processes to log, report on and monitor any e-security incidents. This will help ensure that any damage is minimised, that services can return to normal as soon as possible and that lessons can be learned to prevent similar incidents from reoccurring in future.
7. Ensure technical protections are in place to detect and prevent malware – any malicious code or content which could damage the confidentiality, integrity and availability of a school's network and IT services. Malware can proliferate in many ways, for example via email attachments, social media, malicious websites or removable media such as USB flash drives. Devices that are taken and used off site (for example, devices used by staff both in school and on home internet connections) can become infected and subsequently transfer infections into the school network.
8. Establish and maintain effective network monitoring: this ensures attacks and other e-security incidents are detected quickly, allowing a rapid and effective response in keeping with defined incident management processes.
9. Ensure strategies are in place to control the use of removable media (for example, USB flash drives and CD ROMs). These can introduce malware either intentionally or accidentally.
10. Ensure secure mechanisms are in place to support remote use of school network facilities by staff and pupils, particularly for devices that are used both in school and elsewhere.

[1] https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility
[2] http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/
[3] http://www.nen.gov.uk/10-steps-to-protect-your-schools-network-a-guide-for-school-leaders/