Network Security Advice

PUBLIC

Schools are often concerned about the security of their network and computer systems. Network security prevents accidental damage, loss of data and malicious activity.

The following ten steps are important to keep your school system safe for pupils and staff, and to prevent unauthorised use.

1. User Awareness

The majority of security issues occur or are exacerbated by poor practices, lack of awareness, and lack of reporting.

Provide staff with basic cyber security training.

Review and reduce the numbers of outdated files and emails on servers.

Ensure there is a mechanism for staff to report security concerns promptly and that this is well communicated to stakeholders.

Passwords should be a minimum length of 8 characters, further advice is available from the National Cyber Security Centre.

2. Check Access Controls and Privileges

School staff given IT access are classed as users. Users should only be given the access that they need, not less nor more. If given access which is too restrictive then this will impact on their ability to fulfil their role. If given more access than they require this may provide a chance for criminals to exploit and damage the school network.

Administration accounts are those which enable users to be added, deleted, or modified. It is important that a member of school senior leadership / administration management has access to the administrative account in addition to any technical staff. It is important that the school takes ownership of their own network. These accounts must be controlled and monitored more than all others because they hold high privileges and full access.

All of the user accounts should be protected and monitored for any suspicious or unusual activity.

Have a documented process in place to provision users, which includes approval for the access granted.

Review users on a regular basis to ensure access is still relevant and necessary.

3. Backup Services

The school should have a clear idea who is responsible for scheduling, running and verifying (checking) the backup.

If the school chooses a supplier to fulfil this need a signed contract should be in place, the supplier must be registered as a data processor with the ICO, and service levels and data retention should form part of the agreement.

Remember that data stored in the cloud (such as using Microsoft Office 365 / Google Drive) is not the same as having a cloud backup.

4. Implement a System Recovery Plan

In times of adverse situations such as a disaster, like floods, fire, and theft, a school needs to be ready with a recovery plan to take care of employees, equipment, ensure mitigation / damage limitation and keep the school functioning.

A recovery plan must be created, reviewed, and tested at regular intervals.

Cyber-attacks can also prevent access to all or part of the network or school systems. In the event of a suspected attack schools must report to the police via Action Fraud (0300 123 2040) and consider whether they need to report a breach to the Information Commissioners Office (ICO).

5. Upgrade and Update Software

Schools should upgrade and patch the systems and software as soon as updates are made available or released, and not longer than 14 days after.

It is a good practice to automate the upgrading process from the school server. This means that the upgrades run at a set date / time. A manual process might get postponed by staff or forgotten.

Cyber criminals are consistently attempting to exploit vulnerabilities which patches are designed to address. Verified updates are always signed and will be shared securely from protected website links.

6. Actively Manage Software and Check Software Signatures

The school should review software installed, the list of users with access and the administrators of each system. Users should ask to remove unnecessary software or access that is no longer required as keenly as requesting additional access.

A list of installed software, licensing details, administrators and a list of reliable certificates should all be maintained.

The software that is being used should not be altered or modified in any way and this means it will be properly *signed*. If by any chance, altered or unsigned software is used, it may expose your systems to hackers.

7. Firewalls, Anti-Virus and Malware Protection

Firewalls should be enabled and active on all devices that connect to the internet.

Invest in a strong virus / malware detection solution which provides alerts to users. Ensure that you understand who has oversight of any dashboards or monitoring so that senior leaders can act promptly, when a significant security alert is received.

All devices which connect to the internet should be protected by antivirus and malware protection. This should be set to automatically update, and school policy should prevent users from continually delaying updates or scans.

The school network should have filtering which looks for and reports suspicious activities.

Often the protection is not fully capable of blocking, detecting, and removing threats from the systems, especially if the attack is targeted and sophisticated. Staff need to stay vigilant and report any suspicious or unusual network activity.

8. Networks and Hardware

Ensure that new installations and hardware meet the minimum standards as laid out in Derbyshire Audit's Procurement Guidelines. Security settings, firewalls, and anti-virus (if relevant) must be fully configured before systems are commissioned and in use by staff.

9. Use Encryption

Ensure that all devices have full disk encryption and use encryption when emailing any personal data. Consider whether email communication is the most effective and secure method of transmission.

Backups and any removable drives should also be encrypted.

10. Cyber Essentials Certification

Every organisation must start somewhere, and the basic yet effective controls described in the Cyber Essentials scheme are a good place to begin.

Cyber Essentials is a UK government scheme supported by the NCSC (National Cyber Security Centre). It is a straightforward framework which helps your school or academy to improve its cyber security and understand the key controls which can be used to maintain security, whatever the size.

Cyber Essentials provides a baseline in cyber security which focuses on five key measures (also called controls), which are simple to put in place yet protect organisations from around 80% of common cyber-attacks.

Achieving Cyber Essentials certification helps evidence your commitment to cyber security and documents the fact you have implemented effective protection.

If you would like to discuss support for Cyber Essentials please contact cybersupport@derbyshire.gov.uk

Successful certification will also provide your school with free cyber liability insurance.