SECURITY OF SCHOOL DATA AND INFORMATION: SAFETY FIRST

CONTENTS

SECURITY OF SCHOOL DATA AND INFORMATION: SAFETY FIRST

How do you keep abreast of changing threats and security measures? How often should you run anti-virus software and how do you choose one? Are the security measures you take to protect the personal data held on students and staff robust?

All schools rely heavily on their computer systems and data security is about keeping information safe from damage, loss or theft. It is considered to be best practice for any organisation to exercise the same degree of rigour in assessing the risks to its information assets as it would to legal, regulatory, financial or operational risk. Cyber security is about protecting your computer-based equipment and information from unintended or unauthorised access, change or destruction. You can never be totally safe, but most online attacks can be prevented or detected with basic security practices for your staff, processes and IT systems. There is a risk to your IT services and information wherever they are stored, whether held on your own systems and devices, or on third-party hosted systems (the cloud).

Threats could be posed by people with criminal intent, by accident or through negligence. Current or former employees or people you do business with could have malicious intent. Threats to data security could specifically be posed by or arise from:

- Faulty disks, disk drives, or power failures
- Accidental deletion or alteration of files, e.g. by staff
- Computer viruses
- Unauthorised deletion or alteration of files, e.g. by disgruntled staff
- Hacking
- Destruction by natural disasters such as fire and flood
- Theft of or unauthorised access to computers, laptops, tablets and mobile devices

- Remote attack on your IT systems or website
- Attacks to information held in third party systems, eg your hosted services or school bank account
- Gaining access to information through school staff

An attack could result in financial losses from theft of information, financial and bank details or money; costs from cleaning up affected systems and getting them up and running again; cost of fines if personal data is lost or compromised, or possible damage to other organisations and suppliers.

School leaders need to gain an understanding of the importance of protecting database systems, the growing internal and external threats to an organisation's information and the impact of government regulations on the protection of data. Schools should adopt database security best practices to prevent sensitive student and corporate information being compromised. To understand the threats posed to their information and how best to secure systems and hardware, the school either needs in-house expertise or to buy it in. Up to-date advice is necessary on risks to data in relation to potential internal and external database threats.

DATABASE SECURITY

- Use a password policy
  - Enforce password changes on a set period
  - Make sure no default passwords are left set
  - Use strong passwords
  - Admin accounts should change password more often than general users
- Use the least privilege security model
  - Only provide the privileges an account needs to do the work required
  - When user's roles change the privileges must match the role
- All access must be through an authenticated login
- Rename, lock and expire default accounts

- Apply all security patches for the host operating system and the database system.; if possible harden the operating systems (OS)
- Restrict anonymous access as much as possible; where possible do not allow at all
- Any batch jobs must not have user ID or passwords within then
- If possible encrypt the network traffic using certificates

Schools need effective risk management and governance, and policies and procedures to protect the personal data held in emails, faxes; staff training and through actions such as shredding all confidential paper waste and checking the physical security of premises. Measures that can be taken to keep data secure include:

- Promote a risk management culture.
- Take regular backups of files (backup copies should be stored in fireproof safes or offsite). Every users can set this up as an activity for the IT Manager, so that an audit trail of such backups is created and so that it is not forgotten.
- Protect against viruses by running anti-virus software.
- Use a system of passwords so that access to data is restricted.
- Safely store important files on removable disks, eg locked away in a fireproof and waterproof safe or off-site. Of course Every users have unlimited off-site secure document storage, too.
- Allow only authorised staff into certain computer areas, eg by controlling entry to these areas by means of ID cards, magnetic swipe cards or other devices
- Always log off or turn terminals off or lock them.
- Avoid accidental deletion of files by write-protecting disks or files.
- Use data encryption techniques to code data.
- Ensure third-party managed IT services have security controls in place - check contracts and service level agreements.
- Remove any software or equipment that you no longer need
- Delete data before disposing or re-allocating equipment. Every Asset Management users can set up check boxes for this, so that this is prompted on disposal or re-allocation of IT assets, and so that audit trails are created.

- Review and manage any change in user access, such as the creation of accounts when staff arrive and deletion of accounts when they leave.
- If your school system is disrupted or attacked, ensure that the response includes removing any ongoing threat such as malware, understand the cause and review security.

PORTABLE DEVICES AND STAFF/STUDENT POLICIES

When staff and students either work from home or elsewhere on mobile devices, ensure that suitable measures are taken to protect laptops and tablets and the systems on which the data is stored.

- Write and publish a written policy so that all staff or students are clear on their responsibilities, e.g.
  - If possible mobile device should be encrypted.
  - Do not leave devices visible when away from the car
  - Do not allow non-employees to access devices
  - Do not connect to public Wi-Fi
  - Use encrypted Wi-Fi traffic eg WPA2
  - Do not use third party USB devices
  - Secure home routers
  - Change default passwords
  - User higher WIFI security level
  - Change the default SSID
  - If possible assign static IP addresses
  - Install and keep up to-date antivirus, firewall and malware software
  - Have an automatic partial antivirus sweep of the device on start up or daily
  - Have a full antivirus sweep of the device weekly
  - Keep device patches up to date

ANTI-VIRUS SOFTWARE

How often should you run anti-virus software and how do you choose one?

- Antivirus, firewall and malware software should be running all the time; this is known as "Real Time Protection"
- An antivirus and malware sweep should happen daily; usually at or just after start up; this would be a partial sweep
- A full sweep should take place at least once a week
- Antivirus, firewall and malware software can usually be bought as a single product
  e.g. Sophos, MacAfee, Symantec, Microsoft
- If possible the product should be centrally managed by the school or a supplier

Keep up to-date with advice:

- Have a support contract with the vendor of the system/application.
- Read the vendor advisory notices for your system/application.
- Apply all patches relevant to your system/application.
- Relevant staff should keep their training up to-date as possible for the systems/applications they support.

DATA PROTECTION ACT

If you handle and store information about identifiable, living people –school pupils, students and staff – you are legally obliged to protect that information under the **Data Protection Act 1998**. As an employer the school is obliged to protect employees' personal information. Your pupils and students have a right to see their personal information. They can make a subject access request to see the personal information you hold about them. Students and parents have the right to see their educational records. If the school intends to publish examination results in the media, pupils and students must be informed first.

The Protection of Freedoms Act 2012 places controls on the use of biometric systems in schools, such as cashless catering, access security or borrowing library books. The provisions in the act took effect from 1 September 2013. The DfE has produced guidance on the requirements of the act, such as notification and obtaining parental consent.

The Data Protection Act does not prevent parents and teachers from taking photos of events such as the Christmas play or sports day – asking permission to take photos is normally enough to ensure compliance. If the educational establishment you work in is a public authority, the Freedom of Information Act means you must produce a publication scheme, which outlines the information you will routinely make available to the public - such as minutes of meetings, annual reports or financial information. The Information Commissioner's Office (IOC) publish guides for schools appropriate for different parts of the UK on what information they need to publish. The act also means you must disclose official information when people ask for it (unless there is a good legal reason for you not to) and you must reply within 20 working days.

Schools must notify the ICO that they are processing personal data. Refer to a useful ICO questionnaire "Protecting Personal Information" published in 2013. Their website provides guidance on:

- Notification of purposes for processing of personal data
- Fair processing – let pupils and staff know what you do with the personal information you record about them. Make sure you restrict access to personal information to those who need it
- Security – keep confidential information secure when storing it, using it and sharing it with others
- Disposal – when disposing of records and equipment, make sure personal information cannot be retrieved from them
- Policies – have clear, practical policies and procedures on information governance for staff and governors to follow, and monitor their operation
- Subject access requests – recognise, log and monitor subject access requests
- Data sharing – be sure you are allowed to share information with others and make sure it is kept secure when shared
- Websites – control access to any restricted area. Make sure you are allowed to publish any personal information (including images) on your website
- Installing CCTV for security purposes – inform people what it is being used for and review retention periods - capturing and/or recording images
- Images of identifiable individuals is processing personal information
- Photographs – if your school takes photos for publication, mention your intentions in your fair processing/privacy notice
- Processing by others – recognise when others are processing personal information for you and make sure they do it securely

- Training – train staff and governors in the basics of information governance; recognise where the law and good practice need to be considered
- Freedom of information – after consultation, notify staff what personal information you would provide about them when answering FOI requests

SOCIAL MEDIA

Facebook, Twitter and other social networks make it easy to communicate and share personal information. They can, however, represent a minefield for schools with bullying and the publishing of information that the school would rather not want shared (e.g. photos of horrible school dinners!). It is in the interest of suppliers that these products are available in schools and they should co-operative in providing the support needed to keep them there. Lesson plans for teachers is available from IOC. Protocols for the use of devices and access to social networks will be available in a forthcoming separate guide from Every.

FURTHER INFORMATION AND ADVICE

The Information Commissioner’s Office

The Information Commissioner’s Office (UK independent authority upholding rights in the public interest www.ico.org.uk) provides current legal requirements, guidance, videos and toolkits on data protection).

Get Safe Online

Get Safe Online is a jointly funded initiative between several government departments and private sector businesses.

Their website provides practical advice on how to protect computers and mobiles device against fraud, identity theft, viruses and many other problems encountered online. It contains guidance on many other related subjects too – including performing backups and how to avoid theft or loss of your computer, smartphone or tablet. The site also keeps you up to date with news, tips and stories from around the world.

www.getsafeonline.org/businesses