Data Protection and Cyber Security: what we all need to know

The information below is a summary of the key points raised during the session. It is not designed to be an exhaustive list of procedures, or a guide to GDPR compliance. Please note this is general information and is not legal advice. Please see disclaimer below.

What is Data Protection?

Control over access to and use of personal data stored on computers or in an organised filing system (which can include paper.)

What is Cyber Security?

Protecting our networks, computers, programs and data from attack, damage/loss and unauthorised access.

What is Personal Data?

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. **Article 4 of the GDPR**

The Data Protection Officer and Data Protection Policy

Any establishment defined as a 'public body' should have a Data Protection Officer (DPO). Schools and settings should have a policy that includes the protection of data. Anyone that comes into contact with data held by the school should have read the policy and signed any necessary agreements.

Steps we should all take to protect data

- **Online resources (e.g. web-based curriculum resources) and Cloud storage services.**
  Do not sign children or adults up to online services without consulting your Data Protection Officer. The school should check the privacy policy and note where the data is held (e.g. is it within the EEA?) The school must be satisfied with the steps the service takes to protect the data. The Data Controller (the school) will need a written agreement with the Data Processor (the online service.) Separate parental permission may be required for children to use the service. See the DfE list of suppliers that have self-certified, within this document: https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act (see page 12/13)
- **When sending emails.**
  Do not send standard emails containing personal information. The safest way to do this is through a secure system such as SchoolsFX. If not using such a system, personal information should be encrypted within an attachment, and the password to unlock the file should be communicated separately, not within the same email. Info on SchoolsFX can be found here: http://www.thegrid.org.uk/eservices/schoolsfx.shtml. Do not send links to a file that contains personal data on a cloud service. Always double-check you are sending emails to the correct recipient. Consider disabling auto-complete in address fields.

Steps we should all take to protect data (continued)

- **When carrying personal information on memory stick and other portable drives.**
  Any portable disks that contain personal information should be encrypted.
- **When carrying personal information on laptops.**
  The laptop should also be encrypted so that an additional password is required to decrypt the data.
- **Keeping a clear desk.**
  Do not leave papers that contain personal information lying around unattended on your desk, by the photocopier or anywhere else. Lock the information away when not in use.
- **When taking paperwork offsite.**
  Papers that contain personal information cannot be encrypted in the way a disk can. So avoid it where possible. Where papers must be taken offsite, protect them as best you can, for example by using a lock on the bag that carries them. Consider a signing in/out system so that all papers can be accounted for at all times.
- **Printing unnecessarily.**
  Because paperwork cannot be encrypted, avoid printing documents that contain personal data unless it is absolutely essential.
- **Shredding**
  Always shred paperwork that contains personal information, when disposing of it. Don't use shredded paper as packaging.
- **Not storing data in a physically secure way.**
  Disks, backup tapes, papers etc. that contain personal information should be kept physically secure when not in use, e.g. locked away.
- **When disposing of IT equipment.**
  Always use an approved disposal organisation. Make sure you have a written agreement in place with the organisation, and do not just dispose of the assets yourself.
- **When visitors come to the school.**
  Visitors should be signed in and out and supervised where necessary. Think before you hold the door open for someone.
- **Using personally owned equipment for school work.**
  The data controller has no control over the security of your personally owned devices, so it is not recommended that these are used for any purpose where school personal information may be accessed, stored or used. Only use school-issued devices.
- **Position of monitors.**
  Think about whether computer displays in the school can be seen by people external to your organisation. Can a teacher's monitor be seen from outside the window, or the school office screen be seen from reception, for example?
- **Locking computers and logging out.**
  Get into the habit of logging out of systems when you are not using them, and locking your computers when away from them. School devices should be set to auto-lock if they are not used for a period of time.
- **Applying passcodes to mobile devices.**
  School-owned mobile devices should be set to auto-lock and have a passcode enabled to gain access. Personally owned devices should not be used for work purposes.
- **Passwords.**
  Never share your password. See below for more information on password security.

- **Giving out personal information over the phone.**
  Be very careful when giving out personal information over the phone. Carefully check the person's identity (e.g. through a call-back) and if necessary, don't give the information over the phone, provide it in another, more secure way (e.g. SchoolsFX.)
- **Chit-chat.**
  Always be mindful of who you are talking to, both offline and on, what information they have the right to access, and who might be able to overhear or see your conversation.
- **Back-ups.**
  Information should be backed up, but the same data protection procedures should be applied to the backup as the original.

Steps we should all take to lessen the risk of a cyber-attack

- **Phishing**
  Phishing emails and instant messages attempt to trick us into imparting information such as usernames, passwords, banking details etc. To lessen the risk of being a victim of phishing or other email-spread cyber-attacks:
    - Were you expecting the message?
    - Is the salutation in your actual name?
    - Is it asking you for sensitive information, to follow a link, to log on to something, download something or open an attachment?
    - Which address is it coming from?
    - Is the spelling, punctuation, language and grammar correct?
    - Is there a sense of urgency in the message (e.g. 'Act now')

  If in any doubt, do not click.

- **Malware** (viruses, trojans, worms, ransomware etc.)
  Malware is malicious software inadvertently installed onto computers. To help avoid an infection:
    - Do not click on pop-up windows, banners etc. when browsing the web.
    - Do not open email attachments unless you are 100% sure what it is.
    - Avoid 'click-bait'
    - Keep your anti-virus software up to date.
    - Keep your browser software up to date.
    - Avoid file-sharing services.
    - Use a mainstream search tool.
    - Do not plug your portable media into untrusted computers.
    - Do not plug untrusted portable media into your computer.

- **Password Security**
  It is important to have a strong password, that is never shared. Passwords should be changed regularly, but not so regularly that you need to write it down or just change the number on the end of the password.
    - Do not use the same password for everything
    - Do not use single 'dictionary' words.
    - Do not use easily guessable words (pet's name, child's name etc.)
    - Use special characters, e.g. #~$& etc.
    - Combine upper and lower case characters.
    - Try making up a nonsense word or phrase from the first letter of each word in the line of a song or poem, or by combining random words.
    - When you change a password, really change it, do not just append the next number.
    - If you must write it down, which is not recommended, encrypt the document you wrote it in or, if on paper, lock that paper away.

- **Telephone Scams**
  Be aware that scammer may use the telephone to call you, pretend to be someone else and ask for information or tell you they are emailing an important attachment or suchlike, which you should open immediately. Be cautious on the phone, just as with other methods of communication.

- **Online banking and work with personal data etc.**
  Do not do online banking or use your school device on public wifi networks. Avoid saving your bank details to a website when offered. When doing secure actions online, e.g. banking, look for 'https' and/or a padlock symbol in the address bar. 

- **Social Media**
  Scams and malware may be communicated through social media platforms. When using social media:
  - Think before you 'like', share or copy/paste a status. The post may not be genuine and an attempt to 'farm' likes and shares, or spread fake news etc.
  - If it seems too good to be true, it almost definitely is. Do not click on amazing offers etc.
  - If a post from a friend seems out of character, do not click on any links etc. attached to the post.
  - Think twice before doing quizzes or playing games. Do you really need to do this? It might be an app that can harvest your data or install malware.
  - Avoid 'click-bait' with sensational stories etc. They may lead to malware etc.

- **Staying Aware**
  You can download and print free awareness posters and stickers from the ICO website. Place these around the school as reminders. E.g. near the copier, in the office, on the back of the toilet door, on the bin, by printers etc. Move them around from time to time or they'll become 'invisible'.
  - Download from: https://ico.org.uk/for-organisations/resources-and-support/posters-stickers-and-e-learning/

Further information from the Information Commissioner's Office (ICO) on data protection.

https://ico.org.uk/for-organisations/education

Disclaimer:

The information above should be considered general information only. It is not legal advice and was not written by a legally qualified person. Herts for Learning Ltd. does not warrant that the information contained in this material is correct. In no event will Herts for Learning Ltd. be liable for any loss or damage including, without limitation, indirect or consequential loss or damage, or any loss or damages whatsoever arising from use or loss of use of, data or profits arising out of or in connection with the use of this information.