Data Security - Guidance for schools

Why should your data be secure?

One of the 8 principles of the Data Protection Act specifies that the data must be kept securely.

What data should be secure?

For ease of understanding your data we have given some examples of data and the security measures required to protect them. The examples given are just that, they are not exhaustive lists and the security required depends on the volume of data as well as the sensitivity. For example, the medical records of the whole school require different security considerations to the medical records of a single pupil.

The following categories are for demonstration purposes only.

Red data (those that contain very personal details)

- IEPs
- Education Psychologist reports
- Education Welfare Officer reports
- Medical records
- Personnel records
- SEN registers
- Accessing your Management Information System or admin servers

Amber data (data that contains personal data that if lost could identify individuals)

- Names and Addresses
- Parental contacts
- Pupil reports
- Exam results

Green data (data that does not identify individuals)

- Lesson plans
- Class lists (only showing initials and forenames)
- Curriculum plans
- General marking

If you don't mind it being available on a website or in the local paper then it is green data.

How do you protect your data?

Data should only be accessed by those that are entitled to do so. When data is transported or shared it should be in a way that is appropriate to the sensitivity of that data.

Secure Data Transfer
There are several tools recommended by the DFE for secure data transfer. School use both of these regularly probably without realising what they are. S2S is used to secure pupil data transfers both between schools and schools and LAs. It is used for formatted pupil data but can also be used for other files if encryption is used.
Anycomms or AVCO is used for BHCC to school and school to BHCC transfers. This is a largely automated process that is not suitable for ad-hoc transfers.

- Red, Amber and Green data may be transferred using secure data transfers.

Email

- Red data should never be sent by email. This can only be sent by secure or GCSx email which is not available to schools
- Amber data should never be sent outside the council network so only to brighton-hove.gov.uk and brighton-hove.sch.uk addresses. This is one of the most difficult areas especially because some school email systems using brighton-hove.sch.uk are not hosted within the council network. Email can be forwarded on to any email address which makes it potentially insecure.
- Green data can be sent by email

Please note that if you use a personal email account for school business then be aware that that any information you send is being transmitted across the public internet. You could also find that under Freedom of Information or as part of an investigation, you would need to give others access to your personal email account.

Mobile email
If you use a browser to access email on the move then the above advice applies.

If you use an app on a mobile device to access school email then you need to consider the following additional advice.

- Does your device lock automatically if you leave it unattended and need a pin code to unlock it?
- Does it encrypt email stored on the device?
- Can it be remotely wiped if you lose it?

It should meet all these criteria if you send or receive any email that contains Amber data.

USB sticks
Please note that portable memory devices such as USB sticks should only be used for temporary data storage. They are ideal for moving data around but that data should always be stored somewhere else.

- Red data should never be saved on or transferred by using USB stick.
- Amber data may only be stored on encrypted USB stick.

- Green data may be stored on and transferred by USB stick.

Laptops

It is best practice not to store data on your laptop at all. If you must store data then please consider the following advice.

- Red and Amber data may only be stored on a school owned laptop that is encrypted.
- Green data may be stored on an un-encrypted school or personal laptop.

Cloud (Internet) storage

The best practice for sharing of data for collaboration or marking is to use your VLE. Cloud services such as Dropbox, Google drive and Skydrive should not be considered secure and should only be used for individual use with appropriate data. Some services offer no virus scanning and there is no tracking if you share files with others. If you do use these services, please consider the following advice:

- Red or Amber data should not be stored on cloud storage.
- Green data may be stored on cloud storage.

Remote Access

The School ICT service provides a facility for secure remote access to data held in school. There are 2 services provided. Service 1 allows file access using a personal computer and Service 2 allows file and SIMS/FMS access but requires a school laptop.

- Green data may be accessed on School ICT Remote Access Service 1
- Red and Amber data may be accessed on School ICT Remote Access Service 2

Passwords

Staff who can access sensitive data should consider the security of their password. It must be known only to them selves and be chosen so it could not easily be guessed.

- Staff accessing Red and Amber data must have a complex password
- Staff and other users accessing Green data should use a complex password but may use a simple password

SIMS Data access

Staff must only able to access the data that they need to do their work. Class teacher should only be able to access the data for their class. Passwords must not be shared between users.

Personal laptops/devices in school

Schools should decide whether they want staff to have their personal devices such as phones connected to the school network. Head teachers should decide each case based on need and the sensitivity of the data that may be accessed.

Personal laptops should not be connected to the school network.

Cameras and videos in schools
Pupils and staff should only be filmed or photographed using school owned cameras and these should not be taken home by staff. For further advice including events and performances please see the ICO advice http://www.ico.gov.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Practical_application/TAKING_PHOTOS_V3.ashx

How can School ICT help you with your data security compliance?

- Audits of server to check who has access to what files
- Audit of SIMS permissions to check who has access to what data
- Enforcement of secure passwords and screen locking
- Remote access service for secure access data away from school
- Procurement of encrypted memory sticks
- Encryption of staff laptops (this is work in progress)
- Secure encrypted backup for server data
- Assessment of mobile devices for compliance
- Secure recycling and disposal of ICT equipment