Questions

What is personal data? - Personal data is information that identifies an individual and if lost or mislaid could cause harm or distress. In the school context this could be the name of a learner and their National Curriculum level, their allergies, SEN information, reports – anything where individuals can be identified. Your own data is also personal data so care also has to be taken with staff addresses, phone numbers etc. Personal data can be in electronic or paper format.

Is a picture personal data? Can we put pictures on walls and websites? - As a picture of a learner's face can identify an individual the safest stance is to say that a picture is personal data. However as with all items of personal data you can ask permission to use it in specified ways. Most parents/guardians are quite happy for you to use pictures for stated reasons.

Can parents take photos of their children at school events? - Parents/guardians can take pictures/videos of the children at school events for personal use. Some schools choose to add a statement to letters asking that no pictures including other children be taken or posted on social network sites.

What is the safest way to access personal data? - The best way is to access a specially designed data store such as the Somerset Learning Platform. This can also be completed by using remote access into the school fileserver. Either way the data stays in one place and is not moved.

Why do I need to use an encrypted memory stick and what is it anyway? - If you need to move personal data from one device to another then you can use a memory stick or a removable hard drive, but only if no-one else could read the data if you lost it. Unfortunately a password is not enough, you have to also code the data so that only you can read it – this is called encryption.

Does the school laptop that I take home need to be encrypted? - Again the answer is yes – if it is going to have personal data on, it needs to be encrypted, even if you use a unique user name and password. If someone else logged on they should not be able to read the data.

Can I use the school laptop for personal use? - You do not want your personal photos being seen by learners and you also do not want to accidentally send messages about learners to an email address that was in your personal address book. The best way forward is to keep the school laptop purely for school work.

Can I use my own home computer for school work? - There are no problems with using your home computer to do school work as long as you take care. However the school has a duty to make sure that if you access personal data in a secure way. Advice from the school may include statements such as: make sure the virus checking software is up to date; that you do not work where others can see the personal data; you do not save personal data on the computer. The last is particularly true if other members of your family use the computer.

Can I bring my own computer/tablet into school? - The school will have its own rules about this and you should make sure that you know what is in the e-safety policy. It always pays to check both the school and your own insurance policies in case of loss or damage.

Can I use my mobile phone for school business? - Our advice, mainly from a safeguarding point of view, is not to use your mobile phone for school business. It is ill advised to take pictures and you do not want parents or companies knowing your personal phone number. Obviously, if there is an emergency, safeguarding issues take over and you should use your phone.

Should I set my tablet/phone device to access my school email? - Attractive though it is to access your school email on your mobile phone there are issues of accidentally sending personal data to the wrong person and also issues of work-life balance. If you are happy and it is acceptable to your school then do so – but take care.

BY NC ND

The use of IT equipment out of school and Data Protection issues

Outline

The use of IT equipment outside of the School, either owned by the School or personally owned by a member of staff has become an accepted part of working life. The increasing power of mobile phones, tablets, the number and availability of personal computers in homes and the greater use of web based access systems, have increased the need for **additional care** to be taken in how staff use and share data.

The main issue here is the transfer of Personal Data covered by the Data Protection Act. A definition of Personal Data is that **if lost or mislaid it could cause harm or distress** to the individual. This can include the use of **full names, exam marks, reports, lesson plans** and **mark books**. Using this definition, **pictures or images** must be interpreted as being Personal Data even if they have no associated name or tag. It is important to recognise that staff have the same protections for their Personal Data as do the learners.

Under the Data Protection Act **the School has a duty** to make sure that Personal Data is safe and secure. The School **must** give instructions to all staff on how this data is handled and the security measures that are in place on **any** device or in the handling of paper based resources.

Home use of school devices enables teachers to choose where non-contact work is completed and provides equipment for CPD beyond the school day. The school must give instructions on the use of this equipment and compliance with the school policies on use is essential.

Use of 'The Cloud'

The Data Protection Act covers the transfer of Personal Data. If the data is held on a central store and accessed through **secure remote access** then many issues are avoided.

This central store has to be a storage service that has encrypted transmission, high password security and be in the European Union (Principle 8 of the Data Protection Act). The Somerset Learning Platform (SLP) offers this secure service as do other recognised education companies.

BY NC ND

While commercial storage services such as Dropbox are widely used, with the companies stating that they follow the Safe Harbor agreement, it should be noted that this is a voluntary agreement with the storage of data **not being guaranteed** to be within the EU. There are also issues where a user stores their own home documents on the same services. This can lead to a mixing of personal and professional data and the possibility of actions which breach the Data Protection Act. Therefore the LA cannot recommend the use of these services for the storage of Personal Data.

Remote Access

Schools can also enable their users to access the data that is stored on the School fileserver through remote access. There are many solutions for this which usually includes an annual cost to Schools.

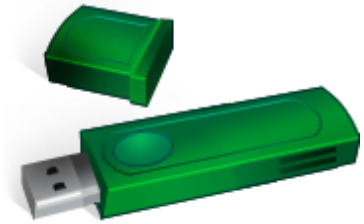
Storage on laptops and other devices owned by a School

If Personal Data has to be stored on individual devices then the area where the Personal Data is stored must be **encrypted**. Encryption is an additional security measure which means that only that user will be able to read the data. Another person who logs onto the computer will not be able to read the data stored in an encrypted area. It is not sufficient for the device just to have passwords or PIN number entry.

- There must be measures in place to make sure that the **virus protection software** is regularly updated to prevent malicious software accessing user names and passwords.
- The use of these devices should only be by the member(s) of staff who has/ have signed out that device.
- Staff should **not register school devices** or services with **personal social networks**. This will avoid the accidental publication of Personal Data such as pictures or images.

Memory Sticks

A common way of transferring data from one computer to another is to use a memory stick or external hard drive. There have been many incidents where these hard drives or memory sticks have been lost or stolen. It is therefore essential that these memory sticks or hard drives are **encrypted** to avoid access to any Personal Data even if they are the property of the member of staff.



CC BY NC ND

Storage on laptops and other devices owned by staff

The School has responsibility for all access to Personal Data. The School must insist that if staff access Personal Data on a home computer that:

- the computer has an up to date **virus checker** to avoid a malicious piece of software gaining access to user names and passwords
- individual **users** are set up on the device
- the computer is only used to access data held in **secure storage**, whether it be in the cloud, through remote access or from an encrypted memory stick
- at no time should **Personal Data** be stored on the device's unencrypted memory or hard drive
- when processing Personal Data this is completed in a **secure** area away from other family members
- it is **locked** if the member of staff leaves the device

Personal Mobile Phones/Tablets

Increasingly the computing power of mobile phones and the mobility of tablet computers are leading to a change in the accessibility to IT. The same principles outlined above apply to these devices.

- the use should be in line with the school's e-safety **policy**
- they must only be used to access Personal Data held in **secure storage**
- the device must have up to date **virus checking** software installed
- they should not be used for **taking pictures** to avoid accidental distribution through social networks and safeguarding accusations
- they should be **PIN protected**
- bluetooth accessibility should be **disabled** when in school

eMail

Many staff now access their school email through a mobile device. In many cases this mobile device will have more than one email account associated with it. This not only presents issues of worklife balance but also Data Protection breeches. Therefore staff should be made aware that:

- they must **PIN protect** any phone used to access their work email
- they must make sure that their phone is **safe and secure** at all times
- they must **never send Personal Data** through accounts that have not been provided by the school
- they should only **'reply' to messages that request the sending of personal data** to make sure that it returns to the correct recipient
- the use of apps or software that allow more than one email account to be registered should be avoided. You should use a **dedicated app** or software for your school account

Reporting Breaches

If at any time a member of staff suspects that there has been a loss of Personal Data they must report it to the schools Data Protection Officer. Failure to do so could result in **disciplinary action**.

CC BY NC ND

eLiM e-learning & information management