An Essential Guide to Data Security for Teachers

by Ian Gover
Introduction

Schools by their very nature store a lot of data. This data can be very personal in nature, detailing medical and personal history as well as other aspects such as attainment and performance. The data stored about a learner is just as valuable as that stored about an adult. Whatever rules and procedures you would like around the data stored about you, should also apply to your pupils.

The main driver behind Data Security must be the school. Schools are no different to other institutions and must make sure that policies and procedures are created and adhered to. They also have the responsibility to train and support staff in applying data security practices.

This guide hopes to lead you through the laws, the issues and responsibilities so that we can all support schools in reaching the highest standards of Data Protection and Information Security.

The structure of the guide is to pose a question and then to explore the answer giving useful links and follow up material.

The questions are:

- What are the laws of the land?
- What is personal data?
- Where can I find out what the school expects?
- Does Data Protection prevent me from being a teacher?
- What materials are there for teaching children about Data Protection?
- Can I use my own computer/tablet to look at pupil’s personal data or school email?
- What is encryption and why is it important?
- How does the Freedom of Information Act effect schools and what information could a school have to publish?
- Can parent’s video school events?
- Can I see the personal data that the school hold about me?
- What information can parents see about their children?
- Can I be sacked if I lose pupils personal data?
- Can I store pupil’s personal data in ‘The Cloud’?
- Can pupil’s photos be displayed on noticeboards?
- Can outside companies process personal data for the school?
- Can I use a personal email address for school business?
What are The Laws of the Land?

The two main laws which address Data security in schools are the Data Protection Act and the Freedom of Information Act. There are other laws which address other IT issues but these deal mainly with criminal activity.

The Data Protection Act\(^1\) controls how businesses or the government uses personal information.

Within this act there are ‘Data Protection principles’. Every business or organisation using personal data must make sure the information they hold is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people’s data protection rights
- kept safe and secure
- not transferred outside the UK without adequate protection

There is stronger legal protection for more sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

Within this Act people have the right to see the data stored about them. There are exemptions that can be applied that cover aspects such as safeguarding but in general all personal data, whether electronic or paper could be disclosed.

The Freedom of Information Act\(^2\) deals with public bodies providing information about the way in which they work their policies and procedures and decisions that they have made. Again there are exemptions to what can be disclosed but these have to be applied carefully.

The main agency for dealing with issues around Data Protection and the Freedom of Information Act is called the Information Commissioners Office\(^3\) - usually shortened to ICO.

Very soon the Data Protection laws will be reinforced throughout the EU and there will be some changes but these are likely to be a little more restrictive and coordinated across all concerned countries.

---

\(^3\) [http://ico.org.uk/](http://ico.org.uk/)
**What is personal data?**

A definition of personal data is:

*Any data or information that identifies an individual that if lost or mislaid could cause harm or distress*

In schools this could include marks awarded for work, comments on MIS systems, behaviour slips, notes in lesson plans – almost everything where there is a named individual.

For example – a teacher places on his lesson plan the initials of those students who receive Pupil Premium. Even though they are not identified by name, combining them with other data or knowledge, someone could identify the individual and if the lesson plan was mislaid could use it to cause distress making this personal data.

The recording of this type of information is good practice and should be encouraged – but the teacher must be aware that the document contains Personal Data and take extra care with it.

Personal Data does not just refer to formal documents but also to notes and other recorded facts – in fact anything held in a formal or informal filing system. As a rule of thumb, if you took the effort to record it then it becomes part of the pupils record.

eMail is thought of as being a communication method but even this is subject to Data Protection and Freedom of Information legislation. If information about a pupil was included in an email then these can be seen as part of the pupils’ record and should be saved in a document library alongside attachments.

**Where can I find out what the school expects?**

All schools have to have policies and procedures to inform staff what to do. One of the statutory policies is one on Data Protection. This can be quite detailed (see SWGfL Template policy⁴) but does list how the school will protect data.

Schools also have to publish Fair Processing notices (Guidance from DfE⁵) for both parents and the workforce detailing what information they store and who they have approved to process the data.

All schools will also have e-Safety Policy (see eLIM Somerset’s example⁶) that will give guidance as to how staff will use technology and this will be linked to an Acceptable User Policy. Staff should always follow the guidance written in these policies.

The school have a responsibility to register with the ICO and make sure that they follow the law. In the way they act as what is known as Data Controllers and have responsibility for the Personal Data

---


⁶ [https://slp.somerset.org.uk/sites/edtech/eSafety/Policies/eLIM%20esafety%20policy%20v2.3.docx](https://slp.somerset.org.uk/sites/edtech/eSafety/Policies/eLIM%20esafety%20policy%20v2.3.docx)
of all the pupils and staff including its use outside of school. This means that it can make demands on staff and tell them how they should use personal data.

These demands must be backed with training. Once this training is complete then if a teacher does something against these policies then they could face disciplinary procedures.

*Teachers must have proper and professional regard for the ethos, policies and practices of the school in which they teach, and maintain high standards in their own attendance and punctuality.* (Teaching Standards)

Once a teacher is aware of Data Security issues they cannot turn a ‘blind eye’. There have been instances where teachers transferred personal data such as names and dates of birth in setting up online learning resources without the knowledge of the school. Although completed for good reasons they may have breached the Data Protection Act. It is up to individual teachers to make sure that everything they do fits in with the schools policy and in this instance permission should have been asked before they set up the resource.

**Does Data Protection prevent me from being a teacher?**

As a teacher you must have access to personal data concerning the children you teach. You would not be able to do your job if you could not. It is not the presence of the personal data or your access that is the problem but the way in which you handle it.

As mentioned in the section ‘What is personal Data?’ almost any information that the school holds about an individual child can be seen as being personal data.

**Taking a register**

When taking a register you should not display the information to the class. If a projector is linked to your computer then make sure that either the screen is frozen before you take the register or that the projector is turned off. The danger is not that the children present in the class know that people are not in the class but that the display might be seen by others passing by the classroom or that information that they should not see is disclosed.

**Mark Book/Lesson Plan Folder**

By the very nature these will hold quite a lot of personal data, some of which will be sensitive in its nature. You are allowed to have these open in the classroom and can leave them on the teachers’ desk will you are in the room. If you leave the room then you should either lock this information away or take it with you.

At night you should always lock away this information or take it home with you. You do not know who will visit your classroom at the end of the day.

**Pupil’s work/classroom displays**

Although you might have marked the work an individual mark in an exercise book would not be seen as being personal data of a type that would cause issues and it would be unreasonable to expect it to be locked away every night.

---

Pupils Photos
Like pupils work a photo can be seen as being personal data. However, like the pupils work they are not sensitive in nature - the pupils know who each other are and other will know that they attend the school. Therefore in areas that are not public there is no real problem in displaying pictures that contain children. If there are pupils for who there are safeguarding issues then the display of these photos might not be advisable.

What materials are there for teaching children about Data Protection?

Everyone needs to know about their rights under the Data Protection and other related laws. This of course applies to learners at school.

There are many resources for older learners with the topic being part of the GCSE syllabus. You can find these by searching the TES site. The BBC site has a very useful resource\(^8\) and the ICO have provided some resources for both primary and secondary learners\(^9\).

One of the richest sources of resources is new events as incidents occur frequently and can be used as discussion points.

Can I use my own computer/tablet to look at pupil’s personal data or school email?

There are dangers in using your own devices for accessing pupil’s personal data or school email. These dangers are mainly around other people seeing the data, whether this is accidental or not, with many computers and tablets at home being shared by other family members.

With your own personal device you will use it to access emails and might set up your personal as well as your school account. It is easy to have the contacts from the school alongside those from friends and family. It is not difficult to see that a slight confusion in names could send an email that holds personal data could be accidentally sent to someone who should not receive that data.

There are also issues with the connections that you might have set on your tablet or computer. It is common these days for tablets to automatically backup photos in cloud storage. This is fine if it is your data, but the use on a field trip could mean that pictures of children could be stored against the Data Protection Act.

The main problem is the sharing of the devices with others. Can you guarantee that others in your family would not look at data that you had shared or email that you receive?

It is up to the school as Data Controllers to set the boundaries of use. They might insist that you only use encrypted memory sticks or only access data remotely. Whatever the school decide the rules they set must be followed.

\(^8\) [http://www.bbc.co.uk/education/guides/z6kj6sg/revision](http://www.bbc.co.uk/education/guides/z6kj6sg/revision)
\(^9\) [https://ico.org.uk/for-organisations/resources-for-schools/](https://ico.org.uk/for-organisations/resources-for-schools/)
What is encryption and why is it important?

Encryption is a term that is frequently heard and slightly misunderstood. Wikipedia states that encryption is the:

'encryption is the process of encoding messages or information in such a way that only authorized parties can read it.'

The key to this definition are the words 'only authorised parties can read it'.

If personal data is shared over the Internet, communications between the person that sends the data and the person (or computer that receives it) have to be encrypted. This is normal practice these days with all the main email clients stating that they have encryption. Most 'cloud' storage is also transferred through encrypted connections.

As well as the lines between computers all devices must also be secure. The ICO have decided that any storage device that holds personal data must be encrypted. This adds an extra layer of security so that only the person who saved the data can see it will be able to read it.

Think about it like this. A school laptop can be accessed by anyone who has a network password. Person A accesses a laptop and saves some files on the hard drive that relate to a medical condition of a pupil in their class and then goes home. Person B picks up the laptop and by entering their password accesses the laptop. Person B will be able to see the file.

Encryption software takes the persons login name and adds another layer of encoding onto the data. Person A can login, write data to a protected encrypted file in the knowledge that if Person B logins they will be unable to access the data.

Many schools have issued teachers with encrypted memory sticks that unless they are opened by a person entering a code (the code might exist on several machines) others will be unable to read the data. If the army personnel that seemingly frequently leave memory sticks on trains used encryption then the press would have less to talk about!

Any laptops used in school as administration machines that have personal data on them must be encrypted, even if they remain in school. The ICO have stated that a laptop counts as a removable device and needs to be treated the same as a memory stick. Of course a thief would never think of taking an ordinary desktop computer would they?

---

How does Freedom of Information affect schools and what information does a school have to publish?

The Freedom of Information Scheme does not concern personal data. It is aimed at providing the public with a way of accessing information about how public bodies are run, making these bodies more accountable to the general public. Schools are no different from other public bodies and have to answer requests for information.

Although no personal data can be released under this act, minutes from meetings, policies as well as financial spending can be disclosed. There are some areas where the information can be ‘redacted’ (black pen drawn through items to censor sensitive information) if the release of this would cause issues.

There is confusion over the difference between a Freedom of Information (FoI) request and a Data Subject Request (DSAR).

Let’s take the common example of a parent wanting to investigate why their child has not been granted support under Special Needs provision. The general policies and procedures that lead up to the decision can be released under a FoI request. The more individual information about the case would be released under a DSAR (see ‘What information can parents see about their children?’).

Information about how money is spent can be released under FoI including some information about salaries. Anyone earning over £60,000 has to be declared and the pay for others (without the direct naming of these people) can be placed in to bands but must be published. Other financial details also have to be published unless there are competition issues.

FoI requests are commonly made by journalists seeking a story and by companies wanting to sell things. Unfortunately, the school had to ignore who has made the request and supply the details within the set time.

Can parents video school events?

This is one of those instances where all the careful work that schools undertake around e-safety and the use of images seems to be in vain. Because of the furore when the Data Protection Act was first introduced there is an exception that allows parents to film their children when taking part in school activities. The act does state that this must be for personal use.

Consider the Nativity Play. If your child was nominated to be Sheep #4 you would want to capture the moment to share with your relatives who could not get to the performance. The Data Protection Act allows you to do this. However other parents may feel uncomfortable if their children are included in the picture. It might be that for this and other safeguarding reasons the school decides that photos or videoing should not take place. This needs to be explained before the event occurs.

Many schools that ban videos/pictures during the performance allow parents to take pictures of their children before or after the performance (alongside other children if their parents have given permission) and this seems to be acceptable. It does seem strange that some schools ban the taking of videos/pictures but then allow the PTA or approved parent to film the exercise and then sell the video to parents.
It is not just the Nativity play in which there have been issues, but also sporting fixtures and community events such as country dancing. Wherever the pictures are taken the issues are around safeguarding and not Data Protection.

The key to work around this area is to work with the parents and agree a way forward before the event.

**Can I see the personal data that the school hold about me?**

The simple answer is you can request to see the information held about you by making a Data Subject Access Request. Details on how can you do this can be found on the ICO website\(^{11}\).

You should be careful how you phrase your request remembering that you might not get data that has been supplied by a third party. There might be information that relates to another person and this might also be withheld.

The school should keep you regularly informed of the progress of your request and provide you with the information in 40 days. There may be a £10 charge for doing this.

In general the school should make every effort to find all the data that relates to you. They cannot hold back any information that might cause them embarrassment.

**What information can parents see about their children?**

Anyone with parental responsibility for a child can make a request to see the data that the school holds about their child. Officially the data belongs to the child and if the school decide that if they are mature enough to understand their rights, then it should respond to the child, not the parents.

Each request has to be treated individually. A child who is in the care of their grandparents or from a broken home might need more careful consideration about the release of data than others.

As for the data that they can have - it is any recorded data that is held about that child. This includes emails and paper documents. The names of other children can be redacted (censored) from the documents but the names of staff that hold post of responsibility should not be.

Obviously elements of safeguarding come into the decision to redact information including instances where the school thinks there could be further incidents against staff outside of school. This applies where people like playground supervisors who have seen and reported an incident live near the family of the people concerned.

\(^{11}\) https://ico.org.uk/for-the-public/personal-information/
Can I be sacked if I lose pupil’s personal data?

It is very unlikely that this would happen, but disciplinary action could take place, especially if you had not paid heed to training and advice. It also very much depends on the type of data, the training you received and how you lost the data.

The school has a legal duty to report any loss of personal data to the ICO making a pre-judgement as to the severity of the issue. The ICO have the ability to tell the school to improve it practices or even in severe cases fine them especially if schools have not improved their practices from previous instances.

Imagine if you lost data that included the medical details of your class by leaving an unencrypted memory stick at an Internet café. If you had received training and had been given access to secure remote storage then there would not doubt be questions asked of your practices. This might end up with disciplinary procedures. However accidentally losing your record book might not even be reported to the ICO.

Can I store pupils personal data in ‘The Cloud’?

‘The Cloud’ is a term that is little understood. It really means that you are using a file server that is located on the Internet - away from the computer you are using and also from any secure local file storage.

This causes issues with the Data Protection Act as the eighth principle states that the data should be kept within the EU. Many of the cloud services either do not do this or use an agreement called ‘Safe Harbor’. This agreement is not a law and could be changed at any time. It is because of this, that the use of ‘The Cloud’ for storing personal data has been discouraged by many companies.

There are versions of cloud services which are secure. The DfE have asked companies to self certificate\(^\text{12}\) and both Google and Microsoft have done this. However it is to be remembered that these are for the services that schools as establishments have created and not the personal version that they also offer. There are also cloud services that can be provided by companies that run VLEs and even by schools themselves that are known to be secure because of information provided in contracts or agreements.

So to answer the question, you can store personal data in the cloud but only on schools approved services.

Can pupil’s photos be displayed on noticeboards?

It depends on what permissions have been given by parent’s and what data accompanies the photo.

If the photo is displayed on a noticeboard for publicity purposes or for the furthering of learning then the agreement that the parents has signed on their child joining the school normally covers this. Again safeguarding takes precedence and if there are any doubts it should not be displayed.

But what about the displays that normally go up in staffroom that illustrate those learners who are not going to get 5A*-Cs at GCSE or those that list allergies? Both of these examples involve sensitive data and although staffrooms are not public places, visitors still visit and can easily see the data.

With the list of allergies parents are normally quite happy to give permission for this information to be displayed but they should be asked.

The display of student’s photos and the exam predictions is against the principles of the Data Protection Act and many parents would probably not give permission for this data to be shown in a public area such as a staffroom. Other ways of sharing this data should be used.

**Can outside companies process personal data for the school?**

The school acts as Data Controller for all the personal data that it uses or creates. This means that it has responsibility for the security of the data no matter where it is.

If the school uses an outside company to process data then it must make sure that the companies processes agree with the Data Protection Act. This is normally indicated within the contract but can agreed with a separate Data Exchange Agreement.

If a school does use someone else to process its personal data it also needs to inform parents of this through the Fair Processing notices13.

**Can I use a personal email address for school business?**

The school must try to make sure that the technology that people use ensures that they prevent breeches of the Data Protection Act.

One of the ways in which it can do this is to make sure that one of the major channels of communication used in schools is secure. They do this by providing an approved email service.

In the question about cloud storage there was a discussion about the storage of data outside of the EU and this also applies to attachments to email. Many personal email accounts store the data outside of the EU. There is also an issue that if you use personal email you might accidentally send an email that contains personal data to a friend with a similar name to someone you work with.

It is for these reasons, and also one of tracking, that mean that many schools have a policy that you only use the school provided email account. Remember, if this is the schools policy, then you have to follow it or face disciplinary action if you do not.