Information Security Guidance for Schools

Document Owner	Michelle hunt Tel: 03000 416286 michelle.hunt@kent.gov.uk
Version	Version 2: June 2018

Data Protection legislation protects personal privacy and upholds individual's rights. A key principle of the GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.

This means that you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. You should remember that while information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures.

The legislation does not define the security measures that you should have in place. It requires you to have a level of security that is 'appropriate' to the risks presented by your processing. You need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing.

This reflects both the legislations risk-based approach, and that there is no 'one size fits all' solution to information security. It means that what's 'appropriate' for you will depend on your own circumstances, the processing you're doing, and the risks it presents to your organisation.

So, before deciding what measures are appropriate, you need to assess your information risk. You should review the personal data you hold and the way you use it in order to assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data was compromised. You should also take account of factors such as:

- the nature and extent of your organisation's premises and computer systems;
- the number of staff you have and the extent of their access to personal data; and
- any personal data held or used by a data processor acting on your behalf.

Here are some basic Dos and Don'ts:

- Lock the office when leaving it unattended for any length of time to prevent unauthorised access to personal information.
- Manual records containing personal information should be locked away in a cabinet or drawer when not in use.
- When documents containing personal information have reached the end of their life dispose of them by shredding or use the confidential waste bins.

- Do not share your user ID or password with anyone.
- If you have a laptop which holds personal data, make sure it is encrypted.
- Ensure that your computer screen cannot be viewed by any unauthorised personnel.
- Do not send personal information by fax unless the information has been de-personalised or the fax machine is a 'safe haven' one (in a secure area, which is locked when unattended).
- Do not send personal information by unsecured email as its security cannot be guaranteed. If it is necessary to send information in this way and you do not have access to secure email, make sure the personal information has been either password protected or de-personalised. Send the data as an attachment to the email and flag as confidential.
- If sending any email to multiple recipients outside of the school, consider using blind copy facility (bcc) so recipients can't view other recipients' email addresses.
- If you are required within the course of your duties to take personal data home (including laptops, videos, etc), do not leave the information unattended for any length of time, especially in a vehicle overnight.
- Do not give out personal information over the telephone; invite the caller to put the request in writing. If the request is urgent take the callers name and switchboard telephone number and verify their details before responding.
- Do not discuss other people's personal business in public areas where conversations can be overheard by people with no right to know the details of the information.
- Refer to the 'Use of Images' policy when making decisions about processing images of young people.
- Remember - at all times treat people's personal information as you would wish your own to be treated.

Transporting information Securely

When there is a need to transport information held within documents, laptops, mobile devices etc, which are of a confidential nature i.e. personal to staff or pupils, or commercially sensitive, it is important to ensure precautions are taken to reduce the possibility of these being stolen.

This is also a requirement of the data protection legislation, which requires data to be kept safe and secure, ensuring that information cannot be accessed by unauthorised persons.

Employees should therefore take all reasonable steps to ensure security is maintained when transporting information between work and home or between work-bases.

Documents and mobile devices should be transported in a way to minimise the opportunity of destruction or loss by ensuring vehicles used to transport them are kept locked and secure particularly when unoccupied.

Car Crime

Many thefts from cars are opportunist crimes of items that may or may not be of value, but are visible to a thief. Thefts can occur whilst stationary at traffic lights,

moving through slow moving traffic or whilst parked in a drive/car park. They do not necessarily have to occur when vehicles are left unattended in badly lit or deserted places.

Opportunist thefts take place anywhere, anytime and often within seconds.

Good Practice

- The best guard against theft of personal information and mobile devices is to avoid having to transport where there is no absolute need.
- Avoid transporting complete files. Only take the relevant documents where possible.
- Do not advertise that you are or will be taking home or transporting items of a confidential nature.
- Ensure that personal information or mobile devices are transported within secure bags, boxes, folders etc to reduce the risk of loss or damage.
- Personal information and mobile devices transported in vehicles should be kept hidden away in a locked boot wherever possible or otherwise kept out of sight to discourage opportunist grab crimes.
- Personal information and mobile devices should not be left unattended even in locked vehicles especially overnight.
- If you can take personal information or mobile devices with you when you leave your vehicle.
- Aim to park in busy, well-lit areas or where there is CCTV coverage to discourage thieves.
- If leaving your vehicle even for a second, whilst paying for petrol, using a cashpoint or just popping into a newsagents, ensure your vehicle is secure and that doors, windows, the boot and sunroof are all locked.

Sharing Information Securely

By Post

If you are sending personal information by post, you must:

- confirm the name, department and address of the recipient;
- seal the information in a robust envelope;
- mark the envelope ‘Private and Confidential – To be opened by Addressee Only’ and place this inside a larger envelope with only the correct name and address on it - this adds an additional level of security as the package is not easily identifiable as ‘valuable’ and administrative staff should only open the outer envelope;

If you are sending **sensitive** personal information by post, you must also:

- send the information by recorded, registered or 'signed for' delivery or by courier where appropriate;
- ask the recipient to confirm receipt; and
- record the disclosure on the service users file
- Registered post is the best way to send sensitive personal or confidential information on an encrypted CD.

Different levels of security can be used depending on the information being sent:

- Reliable transport couriers should be used at all times. Consult with your organisation.
- Packaging must be adequate to protect the contents from damage during transit.

By Telephone
If you have received a request to share personal information via the telephone, you must first confirm that the requestor is who they say they are and has a legitimate reason for access to the information.

Where possible ask for the request to be put in writing or if urgent ask for their contact details. Only accept the main switchboard number of their organisation and confirm with the operator the name, job title, department and organisation of the person with whom you wish to share information. Do not accept a mobile phone number.

Once you have confirmed this:
- do not share information when a return telephone number cannot be supplied - call the practitioner back via the switchboard;
- only provide the information to the person who has requested it - if they are not there you should leave a message for them to call you back;
- do not leave a detailed (disclosure) message with someone else or on a voicemail;
- be aware of who might overhear your call;
- keep a record of any personal information disclosed during the call; and
- record on the service users file the time of the disclosure, the reason for it and if appropriate, who authorised it.

By Fax
Paper documents are often sent by fax. Precautions must be taken when sending personal information by fax because the receiving machine may be sited in an open office, meaning the document is visible to other staff, contractors or visitors. Where possible any information should be shared via a dedicated fax (known as a ‘safe haven’ fax machine).

If you are sending information by fax to a machine that is NOT a safe haven one you must:
- remove any information that could identify an individual
- telephone the recipient of the fax to let them know you are about to send it;
- check the fax number. If the information is confidential ask them to wait by the fax;
- ask the recipient to confirm receipt of the fax; or call them to ensure the fax has arrived;
- use pre-programmed fax numbers where possible to reduce the chance of the fax being sent to the wrong machine;
- ensure that you use an appropriate fax cover sheet. Make sure your cover sheet states who the information is for, and mark it ‘Private and Confidential’;
- ensure you do not refer to the names of the person(s) concerned in the subject heading or on the cover sheet of the fax;

- keep a record that you have sent the fax on the service users file.

By email
Huge amounts of information are sent by email, within and across agencies. Whilst internal messages are generally secure (e.g. within organisations), those sent to external addresses are not considered secure enough for personal information. Personal information must be sent by other methods, some of which are outlined in this section.

When sending personal information via email, you should:

- ensure all recipients need to receive the information - think twice before responding to a group email or copying others in;
- confirm the name, department and email address of the recipient;
- use a flag to mark the message 'confidential';
- do not include personal or confidential information in the subject field;
- ask the recipient to confirm receipt of the email;
- If sending any email to multiple recipients, consider using blind copy facility so recipients can't view other recipients' email addresses

Using password protected files
Password protection and encryption are not necessary for information shared between staff within a secure platform (e.g. within the school) or where secure email is used.

- If you have to send personal information to an external recipient, contain it within a password protected file.
- Remember to use a different password to anything you may use for other tasks because you will have to share the password when you disclose the document.
- Always save the password protected version of the document as a new file and retain the original safely. IT Services will not be able to open password protected or encrypted documents without the password.
- Do not send the password in the same email - preferably ask the recipient to confirm receipt of the information and then send the password in the reply to that email. Or give the password over the telephone.
- Record what information has been sent on the service users file.
- After receiving a password protected file, re-save the information without the password in a new secure place. Do not rely on remembering the password.
- Save an audit trail of your email communications. This could mean saving a copy of all sent and received emails in a separate folder.

Sending information by Secure Mail
When sharing information with other organisations, there are some secure methods available – for example Egress Switch and the **S2S system**.

The S2S system allows schools and local authorities to securely share information, for example to:

- transfer pupil records using the common transfer file protocol (CTF)
- update pupil details with the Learning Records Service (LRS)

- apply for and receive pupil unique learning numbers
- send and receive messages to and from other users within the S2S network.

To send information to another school or local authority, you must:

- use the CTF naming protocols
- save the data in an encrypted folder or file
- send the file as a compressed folder

Full instructions for saving, uploading and receiving files via S2S can be found in the guides for schools and local authorities.

In Person

- Personal or confidential information may be delivered personally by members of staff. Such information may be held in paper or electronic form. Where laptops, PDAs or other electronic devices are used precautions must be taken to ensure the security of systems as well as any data held on the device itself.
- Personal information should only be taken off site where necessary, either in accordance with local policy or with the agreement of your line manager.
- Log any personal information you are taking off site and the reason why.
- Paper based personal information must be transported in a lockable box, sealed file or envelope.
- Electronic information must be protected by appropriate electronic security measures – password or encryption.
- If transferring personal information by car put the information in the boot and lock it, but DO NOT leave in the car overnight
- Ensure the information is returned back on site as soon as possible.
- Record that the information has been returned.

Cloud Computing

Cloud computing is defined as access to computing resources, on demand, via a network. By processing information in the cloud an organisation may encounter risks to data protection that they were previously unaware of. It is important that data controllers take time to understand the data protection risks that cloud computing presents.

Cloud computing is not a one-size-fits-all product and in many cases it can be tailored to fit the specific needs of an organisation. The compliance issues that arise will depend on the type of cloud service in question.

The processing of certain types of personal information could have a greater impact on individuals' privacy than the processing of others. With this in mind, the cloud customer should review the personal information it processes and determine whether there is any data that should not be put into the cloud. This may be because specific assurances were given when the personal information was collected. Often the question may not be whether the personal information should be put into the cloud but what the data protection risks are and whether those risks can be mitigated.

Here is a link to guidance issued by the ICO: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

The guidance includes this checklist to consider:

Risks

- Make a list of the personal information you hold and how it will be processed in the cloud.

Confidentiality

- Can your cloud provider provide an appropriate third party security assessment?
- Does this comply with an appropriate industry code of practice or other quality standard?
- How quickly will the cloud provider react if a security vulnerability is identified in their product?
- What are the timescales and costs for creating, suspending and deleting accounts?
- Is all communication in transit encrypted? Is it appropriate to encrypt your information at rest? What key management is in place?
- What are the information deletion and retention timescales? Does this include end-of-life destruction?
- Will the cloud provider delete all of your information securely if you decide to withdraw from the cloud in the future?
- Find out if your information, or information about your cloud users will be shared with third parties or shared across other services the cloud provider may offer

Integrity

- What audit trails are in place so you can monitor who is accessing which information?
- Make sure that the cloud provider allows you to get a copy of your information, at your request, in a usable format.
- How quickly could the cloud provider restore your information (without alteration) from a back-up if it suffered a major data loss?

Availability

- Does the cloud provider have sufficient capacity to cope with a high demand from a small number of other cloud customers?
- How could the actions of other cloud customers or their cloud users impact on your quality of service?
- Can you guarantee that you will be able to access the information or services when you need them?
- How will you cover the hardware and connection costs of cloud users accessing the cloud service when away from the office?
- If there was a major outage at the cloud provider how would this impact on your business?

Legal

- Make sure you have a written contract in place with your cloud provider.
- How will the cloud provider communicate changes to the cloud

service which may impact on your agreement?
- Which countries will your cloud provider process your information in and what information is available relating to the safeguards in place at these locations? Can you ensure the rights and freedoms of the data subjects are protected?
- You should ask your cloud provider about the circumstances in which your information may be transferred to other countries.
- Can your cloud provider limit the transfer of your information to countries that you consider appropriate?

Information Security Breaches

The Information Commissioners Office (ICO) has the power to issue fines of up to 20million Euros (approx £17m) for serious breaches of the GDPR and the Data Protection Act 2018.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Reporting a breach

The GDPR introduces **a duty on all organisations** to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

A breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

To notify the ICO of a personal data breach, please see their pages on reporting a breach.