Good practice in information handling: Data security dos and don’ts

We have written this guide for anyone working in a school, college or university who collects, manages, transfers or uses data about learners, staff or other individuals during the course of their work. Its aim is to raise your awareness of where potential breaches of security could occur. Following these ‘dos and don’ts’ will help you to prevent data from being lost or used in a way which may cause individuals harm or distress and/or prevent the loss of reputation your organisation may suffer if you lose personal data about individuals.

This document is one of a series of good practice guides to help schools, colleges and universities protect personal and sensitive data. Building on good practice from industry and central government these guides describe procedures and possible technical and operational solutions that can help organisations reduce the risks of data security incidents and comply with current legislation.

Produced by Becta on behalf of the Department for Children, Schools and Families, these guides have been reviewed and updated with feedback from a number of cross-sector organisations including DCSF, DIUS, JISC Legal, The Information Authority and JANET(UK), as well as from schools, local authorities, RBCs and suppliers.

For further information on these guides, please see http://www.becta.org.uk/schools/datasecurity and http://www.becta.org.uk/feandskills/datasecurity.

Your roles and responsibilities

As a member of your organisation you have a shared responsibility to secure any sensitive or personal data you use in your day-to-day professional duties.

Important ‘dos’

- make sure you and your colleagues are adequately trained
- follow guidance
- become more security aware
- raise any security concerns
- encourage your colleagues to follow good practice and guidance
- report incidents.

Why protect information?

Organisations hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this data could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of personal data could result in adverse media coverage, and potentially damage the reputation of your organisation. This can make it more difficult for your organisation to use technology to benefit learners.

What information do you need to protect?

You should secure any personal data you hold about individuals and any data that is deemed sensitive or valuable to your organisation. Your organisation should have someone who is responsible for working out exactly what information needs to be secured. This person is your Information Asset Owner. They should understand what information you need to handle, how the information changes over time, who else is able to use it and why. Several people may share this role if you work in a large organisation.

If you don’t already know, find out who is acting as your Information Asset Owner.

Using protective markings

It is good practice to protectively mark personal data. This will help people handling it understand the need to keep it secure and to destroy it when it is no longer needed. This is especially important if personal data information is combined into a report and printed.

Your Information Asset Owner should help you work out how you need to mark the information you view as part of your job. There are different levels of marking depending on how just how sensitive the information is.

Steps you can take to help prevent security problems

There are plenty of things that you should do (or not do) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these ‘dos and don’ts’ will apply to how you handle your own personal information. Using these practices will help you to protect your own privacy.

We have separated these points into different areas to make it easier for you to refer back to.

Working online

Do

- make sure that you follow your organisation’s policies on keeping your computers up to date with the latest security updates. Make sure that you keep any computers that you own up to date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Get advice from your IT team if you need help.
- only visit websites that are allowed by your organisation. Remember your organisation may monitor and record (log) the websites you visit.
- turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer and attack and forgery site warnings in Mozilla Firefox.)
- make sure that you only install software that your IT team has checked and approved
- be wary of links to websites in emails, especially if the email is unsolicited
- only download files or programs from sources you trust. If in doubt, talk to your IT team.
- check that your organisation has an acceptable-use policy (AUP)[1] for the internet and ensure that you follow it.

Email and messaging

Do

- read your organisation’s email policy[2]

[1] See Becta’s publication *AUPs in Context: Establishing Safe and Responsible Online Behaviours* [http://publications.becta.org.uk/display.cfm?resID=39286].

[2] See Becta’s information on developing e-safety policies [http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_pol_03].

- report any spam or phishing[3] emails to your IT team that are not blocked or filtered
- report phishing emails to the organisation they are supposedly from
- use your organisation's contacts or address book. This helps to stop email being sent to the wrong address.

Don't

- click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on.
- turn off any email security measures that your IT team has put in place or recommended
- email sensitive information unless you know it is encrypted[4]. Talk to your IT team for advice.
- try to bypass your organisation's security measures to access your email off-site (for example, forwarding email to a personal account)
- reply to chain emails.

Passwords

Do

- follow your organisation's password policy
- use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers)
- make your password easy to remember, but hard to guess
- choose a password that is quick to type
- use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password. Change your password(s) if you think someone may have found out what they are.

Don't

- share your passwords with anyone else
- write your passwords down
- use your work passwords for your own personal online accounts

[3] Phishing is an attempt to obtain your personal information (for example, account details) by sending you an email that appears to be from a trusted source (for example, your bank) [http://www.google.co.uk/search?q=define%3A+phishing].

[4] Encryption is a way of scrambling information. It helps stop anyone using the information if they do not have an electronic key or password to unscramble it.

- save passwords in web browsers if offered to do so
- use your username as a password
- use names as passwords
- email your password or share it in an instant message.

Laptops

Do

- shut down your laptop using the ‘Shut Down’ or ‘Turn Off’ option
- try to prevent people from watching you enter passwords or view sensitive information
- turn off and store your laptop securely (if travelling, use your hotel’s safe)
- use a physical laptop lock if available to prevent theft
- lock your desktop when leaving your laptop unattended
- make sure your laptop is protected with encryption software.

Don’t

- store remote access tokens with your laptop
- leave your laptop unattended unless you trust the physical security in place
- use public wireless hotspots – they are not secure
- leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- let unauthorised people use your laptop
- use hibernate or standby.

Sending and sharing

Do

- be aware of who you are allowed to share information with. Check with your Information Asset Owner if you are not sure.
- ask third parties how they will protect sensitive information once it has been passed to them
- encrypt all removable media (USB pen drives, CDs, portable drives) taken outside your organisation or sent by post or courier.

Don’t

- send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives) if secure remote access is available
- send sensitive information by email unless it is encrypted

- place protective labels on outside envelopes. Use an inner envelope if necessary. This means that people can't see from the outside that the envelope contains sensitive information.
- assume that third-party organisations know how your information should be protected.

Working on-site

Do

- lock sensitive information away when left unattended
- use a lock for your laptop to help prevent opportunistic theft.

Don't

- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room.

Working off-site

Do

- only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above.
- wherever possible access data remotely instead of taking it off-site
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any services you have used
- try to reduce the risk of people looking at what you are working with
- leave your laptop behind if you travel abroad (some countries restrict or prohibit encryption technologies).

Further help and support

Your organisation has a legal obligation to protect personal information. Your senior management should be aware of their legal obligations under the Data Protection Act 1998. For more information, visit the website of the Information Commissioner's Office [http://www.ico.gov.uk].

More detailed guidance for organisations can be found on the Becta website [http://www.becta.org.uk/plansustainablesuccess and http://www.becta.org.uk/schools/esafety].

Test your online safety skills at the Get Safe Online website [http://www.getsafeonline.org].