The golden rules of keeping data safe

How would YOU want your personal details handled?

This booklet contains the most important things you need to be aware of and think about to keep data safe – a practice known as information assurance (IA). There is much more detailed information on CABlink **(search/tag 'information assurance')**.

Data security is everyone's responsibility

Whether employee or volunteer, office or home-based, we have all agreed to abide by the Citizens Advice service's guidelines and policies relating to data security and acceptable use of ICT.

Keeping data safe is a legal obligation

Failure to take reasonable care when handling sensitive data can result in a fine of up to £500,000.

Protecting data helps to protect our reputation

A high profile data security incident has real potential to impact on our reputation and ability to secure funding, as well as on the individuals involved.

Everyone should complete IA training

All staff and volunteers should successfully complete basic IA training annually, and always before access to sensitive data is allowed. Some staff in senior roles should complete more in depth training.

In some roles you will be responsible for IA risk assessments

If you are involved in developing products, managing projects or establishing partnerships you will need to undertake an IA risk assessment and, depending on the outcome, may need to adopt a formal IA risk management process.

Do not release sensitive data into the public domain

Data is sensitive if its release – either on its own or in combination with other publicly available data – has the potential to cause harm or distress.

Complete a series of checks before sharing sensitive data with another organisation or individual

- Does the recipient have a valid business need to see it that can't be met any other way?
- Do you have an information sharing agreement in place with them?
- Are you sharing the minimum amount of data required? (Begin with totally anonymised aggregated data, only share more – incomplete individual records, a whole individual record, or more than one whole record – as absolutely necessary.)
- Do you have the legal authority to share the data?
- Do you have the consent of the individuals involved?
- Do you have a secure way to transfer the data that is appropriate to its level of sensitivity?

Avoid storing sensitive data on laptops

It is better to access sensitive data through our secure servers than store it locally on a laptop. If this is unavoidable, ensure the laptop is encrypted to the recommended standard.

Classifying data as confidential

Labelling data in a header or footer to indicate whether it is sensitive gives a clear indication to others about how the document should be treated.

- Not protectively marked (optional) – the material can be distributed freely.
- Confidential – for any sensitive data.

Dispose of sensitive data securely

Contact the IT Servicedesk for advice about laptops and hard drives USB's and CDs; cut and burn audio tape; shred paper.

Choose a strong password

Try thinking of a memorable line from a song you like, for example 'one for the money, two for the show'. Then recreate it using numbers, symbols and mixed letters: 1Ftm2fts. Never share passwords or write them down.

Sending unprotected email is not a secure method of data transfer

Confidential level data may occasionally be sent by email attachment but only if the secure encryption procedure is followed. Also check; the auto-complete function hasn't brought up the wrong email address, who belongs to any group email addresses, the recipient has a secure server.

Be especially careful when faxing sensitive data

It is particularly easy to make a mistake when faxing data. Only do so if there is no other means of sharing it. Double check the number, mark the document as sensitive, ensure there is someone waiting at the other end and ask them to confirm receipt.

Use secure printing where it is available

Some printers have a confidentiality function which means that documents will only come out when you are present and have entered a code.

Only use assured security products and services

If you need a data security-related product or service, search the Communications-Electronics Security Group's database www.cesg.gov.uk or ask the IA Manager for advice.

Some aspects of data security relate to our physical environment

Always wear your identity pass and never lend it to anyone. Report anyone who you think does not have permission to be in the building. Lock your computer while not at your desk, and lock away hard copies of sensitive data when not in use.

Be conscious of data security when travelling or working away

Take the minimum amount of sensitive data needed and keep it with you where possible. Record what you take so it is possible to identify whether anything has been lost, and what. Try not to accidentally disclose any sensitive information in conversation and avoid being overlooked.

Report data security incidents to the Bureau IA Manager immediately, they should contact Bureau Direct

Prompt notification is important so the relevant people (who might include those with information systems, legal and press responsibilities) can work to minimise the impact and preserve any evidence.

See **CABlink** for more details
(search/tag 'information assurance')