

# Information Security

## - A Members' Guide

### Appendix C



## This is an overview of the Information Security at Cambridgeshire County Council for Members.

### Data protection e-learning course for Members - [link](#)

Handling information safely is crucial to enable the Council to comply with legislation such as the Data Protection Act, Freedom of Information Act, Human Rights Act, Computer Misuse Act, Companies Act and Civil Contingencies Act.

The [Safe Information Handling Policy](#) which forms part of the Information Management Policy framework describes:

- how to transport data from one computer to another;
- how to ensure that information is destroyed securely.

**It is your responsibility to ensure that these policies are adhered to.**

### What information do we need to be careful with?

It is important to know the sensitivity of the information which we handle, we categorise information into 2 categories, this are:

- Official - the majority of information.
- Official Sensitive – more damaging consequences on individuals or the Council is lost or unauthorised disclosure
  - e.g. it contains information about individuals such as their address or date of birth.

We need to be particularly careful when we're handling Official Sensitive information.

### What makes a good Password?

The Council's password policy states that passwords must include:

- creating a password of at least 8 characters (preferably more characters) including an upper, lower and numeric or special character; and
- not writing your password down or sharing it with anyone; and
- making your password unique and not easily guessed.

A good password should be:

- a combination of upper, and lower case letters, numbers and special characters; and
- not be something that is easily identifiable to you, i.e. your pet's name.

### Creating and remembering passwords

- use phrases - you can add a number according to which letter you have used and any punctuation. For example, using the phrase "I wandered lonely as a cloud" could become "!W4nd3r3dlonlelyasacloud";
- use codes - turn certain letters into numbers and insert them into a phrase or word. For example "a" becomes @, e becomes 3;
- shuffling - choose a word and a number of the same length, for example "minion" and 456789. Alternate each character to produce a random, mixed password - "@!\*m4i5N6i7o8n9".

### Password Security

The important things to remember are that:

- you must never write it down;
- you must never share it with anyone;
- if you think that someone knows your password, change it immediately.

**It is your responsibility for anything that is done under your user name and password, regardless of whether or not it was you.**

**Safe Information Handling Guidance** states that:

- when out of the office you must maintain the security of any Council information or devices
  - i.e. locking away and not left unattended;
- use follow-me printers/ MFD when printing to ensure security. Stand by the printer and ensure all pages have been printed and collected;
- take particular care in doing so if the follow-me printer/MFD is in a publicly-accessible location;
- if sending a letter or email, check that the address for the recipient is clearly marked and is correct.
- faxing should generally be avoided as it is insecure;
- fax machines must only be used to transfer personal information where it is absolutely necessary to do so and there is no more secure alternative, e.g. secure email.

### **Security incident or breach**

A security incident or data breach happens when there is an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service.

When a security incident/breach happens then this can cause the following:

- loss of trust;
- compensation;
- fines or other sanctions from the Information Commissioner.

When there is a security breach or incident then you must do the following immediately:

- call the police, report the theft and get a crime reference number;
- email [data.protection@cambridgeshire.gov.uk](mailto:data.protection@cambridgeshire.gov.uk) and IT Helpdesk (0300 126 7333) and report the incident;
- assist the Data Protection Officer in the investigation.

For further guidance please contact the Information and Records team [data.protection@cambridgeshire.gov.uk](mailto:data.protection@cambridgeshire.gov.uk)