Protecting confidential information

The council has always taken its obligation to safeguard personal information about its citizens, staff and third parties very seriously. These guidelines exist to remind everyone to exercise good judgment when processing, storing, or disposing of materials that contain confidential information.

Staff should remain aware of the need to protect both:

- structured information (eg in applications such as Framework)
- unstructured information (eg in e-mails or Word or Excel documents).

How do I know if something is confidential?

Information is defined as being confidential if it’s of a personal and/or sensitive nature:

Personal information

Personal information is defined as any details relating to a living, identifiable individual.

Within the council this applies to a great many categories of people:

- past and present staff
- service users
- councillors
- third party organisations.

Information relating to all these people need to be treated correctly and with the appropriate degree of confidentiality.

Sensitive information

Sensitive information is defined as any information which could adversely affect:

- the national or local security interests
- the privacy to which an individual or a group is entitled to.

Within the council this may relate to:

- political confidential papers
- financial or business affairs of a person or organisation
- personnel matters
- commercial and contractual information
- legal advice.

Sensitive information should be handled with care and may require different levels of security measures depending on who needs to access the information.

Guidelines

To prevent confidential information from falling into the wrong hands, the following guidelines should be followed:

- confidential information should always be stored on a secure server protected within the Council’s corporate network and subject to backup strategy.
- Confidential information should only be stored off the council's corporate network if there is justified business case for it and the security of the information can be guaranteed
- users should only be permitted to create, update, enquire on or remove confidential information held on the council corporate network with the agreement of the relevant data owner (or someone delegated by the data owner)
- to prevent unauthorised access to confidential information held on the Council’s corporate network, access should only be provided if:
  - there is individual authentication of users. Individual users have a unique identifier/password to access confidential information
  - there are access profiles. Appropriate access profiles are in place for ensuring that users can access and retrieve only that information that they have a legitimate need to know
  - there are audit logs. Audit logs where possible are kept for users accessing confidential information. This may take the form of a separate log or information within application system records relating to who accessed, what changed and when undertaken
- confidential information held on computers or on other removable media devices should only be discarded if it complies with the council's IT disposal procedure. It should not be discarded in standard trash containers that are open, unsecured, or in public view
- confidential information stored on diskettes, backup tapes or on other electronic media devices should be physically secured with access restricted to authorised personnel only.
- confidential information held on laptops or removable media devices should be regularly backed up onto the council's corporate network drive and kept to a minimum amount. If users neglect this task they run the risk of losing their information if the laptop is stolen or gets affected by viruses, worms and Trojan horses. Viruses can cause irreparable damage to your data
- if confidential information needs to be temporarily copied it should only be done when it is necessary for the business of the council, and saved on a secure computer that requires authentication and/or password protection. All temporary copies must be deleted as soon as they are no longer required
- computers that contain confidential information must be wiped clean (deleted and erased) when they are no longer in use.

Electronic communications

Protection of internal electronic communications

No special protection measures are necessary for sending confidential information within the council's corporate network.

Protection of external electronic communications

Confidential information should only be sent outside the council's network if it can be sent securely. Documents containing confidential information created using Microsoft Office products such as Word or Excel must be password protected using the products own encryption provider with a key strength of at least 128 bits.

For example RC4 Microsoft Enhanced Cryptographic Provider v1.0 with a 128 bit encryption which is available on Microsoft Office products 2002 or later and is considered strong encryption and is widely used, for example by online banking systems and in PDF encryption.

This is sufficiently secure for council purposes at the moment. Naturally the password should not be written on the media that also contains the encrypted files, and should conform to the selection and use of password guidelines.

Responsibilities

It is the responsibility of all staff to abide by these guidelines. Any breach of these guidelines could be dealt with in accordance with the appropriate disciplinary procedures which could result in formal action and could also expose the council to civil and criminal penalties.

Further information

More information is available in the confidential information toolkit [Word].

For further information on protecting confidential information or IT security, please contact the Risk and Change Manager, Sue Horobin