Gloucestershire County Councillors' Information Security Protocol

As part of your role as a Councillor you will have access to Council information. The purpose of this protocol is to set the standards for use of Gloucestershire County Council's information. It will help protect you, the Council and service users from the consequences of accidental loss or disclosure of personal and/or sensitive information, and promotes secure working practices. It will also help protect you and/or the Council against potential fines from the Information Commissioner resulting from accidental loss or disclosure of this information.

As you will have access to, and responsibility for, Council information you must:

Access

1. ensure that your computer has a separate password protected user account for you and the password must only be known to you and kept secure[1];
2. ensure that Council information is not accessed by anyone who does not have a right to see it;
3. ensure the screen of your PC cannot be overlooked;
4. not leave personal and/or sensitive information on display or unattended;
5. not leave your computer logged on and unattended for any period of time, but must either log out or lock the device (e.g. using the Ctrl, Alt and Delete keys) when leaving it unattended for a short period of time;

Protection

6. ensure your wireless connection is secure;

If using your own PC:

7. keep your anti-virus software and software patches up-to-date;
8. enable a firewall on your home PC. More detail on how to do this can be found in Enable your firewall on your home PC

Storage

9. not allow Council information to be stored in cloud based storage (e.g. Googlemail) without prior permission from the Council;

[1] A password should be at least 8 characters long with at least one upper case character and both alpha and numeric characters. Avoid passwords that could be easily guessed or dictionary words as these are more easily hacked. You should change your password regularly.

10. have a lockable filing cabinet or drawer for personal and/or sensitive paper records

Use

11. take care when printing Council information to ensure it is kept secure when in paper format;
12. not auto-forward Council information to your personal email account; manual forwarding can be done if it is appropriate taking into consideration the information the email contains.

Disposal

13. shred personal/sensitive Council information or bring it into Shire Hall for secure disposal;
14. ensure that any personal/sensitive Council information stored on your computer/device is deleted and wiped as appropriate, particularly if the computer/device is sold or transferred to a third-party. Contact the ICT Service Desk on 01452 425999 for help.

Something's gone wrong

15. if you discover a breach of security that affects Council information (e.g. theft of a computer, sensitive information has been sent to the wrong person and so on), you must promptly report it to the ICT Service Desk 01452 425999 or the Information Management Service on 01452 425071 or informationsecurity@gloucestershire.gov.uk.

Information security tips

- Do not open emails or click on the link in an email if you are not confident of the origin. In some cases, doing so may cause malicious software to be downloaded to your computer.
- Avoid entering your GCC email address on non-reputable or non secure websites. This is how SPAM (junk mail) can originate.
- Don't leave laptops or files in your car overnight and if absolutely necessary at other times, lock in the boot.
- Don't do anything to jeopardise the Council's or third parties' confidential information through use of social media, such as Facebook or Twitter.
- We recommend sending information securely to third parties by encrypting personal or sensitive information. More detail on how to do this can be found in Advice about encryption

Information security is not just about technical measures; it also covers the information you have responsibility for. Think about:

- Who are you talking to; are they who they say they are?
- What information are you providing to them; have they been able to get information out of you surreptitiously?
- Where you hold discussions or telephone calls; can you be overheard?
- Where are you reading documents; is someone looking over your shoulder?
- What information you share; is it appropriate and not excessive?