Elected Members' 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 special category (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 you only access your council emails and folders via Blackberry Work
2. ensure that your password is only known to you and kept secure[1];
3. ensure that council information is not accessed by anyone who does not have a right to see it;
4. ensure you cannot be overlooked when working on your device;
5. not leave personal and/or special category (sensitive) information on display or unattended;
6. not leave your device open and unattended for any period of time. Instead you must either log out or lock the device (e.g. using the Ctrl, Alt and Delete keys where appropriate) when leaving it unattended, even for a short period of time;

Protection

7. ensure any wireless connection you use is secure;

Storage

8. not allow council information to be stored in cloud based storage (e.g. Googlemail) without prior permission from the council;
9. have a lockable filing cabinet or drawer for any personal and/or special category (sensitive) paper records.

Use

10. avoid printing council information where possible, but if printing is necessary, ensure it is kept secure when in paper format;

---

[1] See the council's latest guidance on what makes a good password at https://staffnet.gloucestershire.gov.uk/internal-services/information-management-service/cyber-security/passwords/

Information Management Service. May 2021.   Email: informationsecurity@gloucestershire.gov.uk

11. not auto-forward council information to your personal email account; manual forwarding can be done if the email does not contain any personal, special category (sensitive) or commercially sensitive information pertaining to the council.

Disposal

12. shred personal/special category (sensitive) council information or bring it into Shire Hall for secure disposal;

Something's gone wrong

13. if you discover a breach of security that affects council information (e.g. theft of your GCC iPad or personal device, special category (sensitive) information sent to the wrong person, etc.), you must promptly report it to the ICT Service Desk 01452 425999 or the Information Management Service at 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 device. Report any suspicious emails to informationsecurity@gloucestershire.gov.uk
- Avoid entering your GCC email address on non-reputable or non secure websites. This is how SPAM (junk mail) can originate.
- Do not leave electronic devices or files in your car overnight and if absolutely necessary at other times, lock in the boot if you cannot carry them with you.
- 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 at https://staffnet.gloucestershire.gov.uk/internal-services/information-management-service/email-security/egress-switch/

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?