GovConnect Personal Statement

This statement is to ensure that each person using the GCSx is aware of the commitments and security measures surrounding the use of the network. Staff requiring access to GCSx, MUST agree this statement (by completing the GovConnect Security Form) before connections can be made live. Additional guidance can be found on the intranet; https://intranet.warwickshire.gov.uk/adviceandguidance/ICT/InformationSecurity/Pages/SecureMail.aspx .

Security Policies

You must understand and agree to comply with the security policies and procedures of Warwickshire County Council as well as those contained within the Code of Connection. For the avoidance of doubt, the security policies and procedures relating to secure email and IT system usage include:

- Chief Executive's Information Security Policy Statement
- E-mail and Internet Code of Practice
- WCC Protective Marking, Handling and Disposal Policy
- Guidance Note for GCSx Users – Government Security
- Warwickshire County Council – Public Interest Reporting Code
- Staff Briefing - Data Protection Act 1998

GovConnect Statement

You must agree that you;

1. acknowledge that use of the GCSx may be monitored and/or recorded for lawful purposes
2. are responsible for any use of the GCSx using your unique user credentials *(user ID and password)* and email address.
3. will not use a colleagues credentials to access the GCSx and will equally ensure that your credentials are not shared and are protected against misuse.
4. will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, you will not write down or share your password other than for the purposes of placing a secured copy in a secure location at your employer's).
5. will not attempt to access any computer system that you have not been given explicit permission to access.
6. will not attempt to access the GCSx other than from IT systems and locations which you have been explicitly authorised to use for this purpose.
7. will not transmit information via the GCSx that you know or suspect or have been advised is classified Confidential, Secret or Top Secret.
8. will not transmit information via the GCSx that you know or suspect to be unacceptable within the context and purpose for which it is being communicated.
9. will not make false claims or denials relating to your use of GCSx (e.g. falsely denying that an email had been sent or received).

Govconnect Personal Statement

10. will protect any information sent, received, stored or processed by you via the GCSx as required by the WCC Protective Marking, Handling and Disposal Policy.
11. will not send Protectively Marked information over public networks such as the Internet unless it is encrypted to WCC Security Standards.
12. will always check that the recipients of email messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain.
13. will not auto forward email from your GCSx account to any other non GCSx email account.
14. will disclose information received via the GCSx only on a need to know basis.
15. will not forward or disclose any sensitive or protectively marked material received via the GCSx unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel.
16. will seek to prevent inadvertent disclosure of sensitive or protectively marked information by:
    - avoiding being overlooked when working,
    - taking care when printing information received via the GCSx (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts etc.)
    - and carefully checking the distribution list for any material to be transmitted.
17. will securely store or destroy any printed material.
18. will not leave your computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the GCSx (this might be by closing the email program, logging off from the computer, activating a password protected screensaver, etc so as to require a user logon for activation).
19. where your organisation has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that caused the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then you will not attempt to disable such protection.
20. will make yourself familiar with the security policies, procedures and any special instructions that relate to the GCSx.
21. will inform your manager immediately if you detect, suspect or witness an incident that may be a breach of security
22. will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended.
23. will not remove equipment or information from Warwickshire County Council premises without appropriate approval.
24. will take precautions to protect all computer media and portable computers when carrying them outside Warwickshire County Council premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief).
25. will not introduce viruses or other malware into the system or GCSx and will not disable anti virus protection provided at my computer and will comply with the Data Protection Act 1988 and any other legal, statutory or contractual obligations that are relevant.
26. will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that Warwickshire County Council informs you are relevant
27. if you are about to leave your employer, you will inform your manager prior to departure of any important information held in your account.