

Acceptable Use of ICT Policy

SOUTH WEST WALES CORPORATE JOINT COMMITTEE

1. INTRODUCTION

- 1.1. This Policy relates to the use and monitoring of all of the CJC's IT and communication systems, including telephones, mobile telephones, facsimile machines, computers (including laptops, iPads, smart phones and personal organisers), email, the internet and the intranet.
- 1.2. The CJC provides IT and communication systems for business purposes and the use of these systems at all times is subject to this policy. Breach of this Policy will be considered a disciplinary matter.
- 1.3. This Policy applies to all employees of the CJC, elected members, contractors, agency staff and any others with access to CJC information assets or who use the CJC's IT and communication systems

2. EMAIL

- 2.1 CJC email accounts are provided for work purposes only. Personal email is not to be sent.
- 2.2 All emails sent and received from NPT email addresses are monitored by the CJC and may be read as part of any service review and /or investigation carried out.
- 2.3
- 2.4 Email correspondence cannot be considered private. Emails can be easily intercepted, copied, forwarded and stored without the original sender's knowledge. You must take into account the fact that any email sent may be read by a person other than the intended recipient.
- 2.5 Any attachments sent to external email addresses which contain personal or sensitive material should be encrypted or password protected unless a secure e-mail system i.e. Criminal Justice Secure eMail (CJSM) is used. Advice on encryption can be obtained from the Monitoring Officer.
- 2.6 All messages and files are automatically scanned for viruses before being introduced into the network, but this does not provide a complete guarantee of protection. All employees have an obligation to be cautious when opening emails and attachments from unknown sources.

- 2.7 Contracts can be entered into by email in the same way as they can by letter or on the telephone. You must at all times take care to ensure that you do not inadvertently enter into contracts by email which bind the CJC, and you should be aware that contracts must only be entered into in accordance with normal contract procedures.
- 2.8 You must not under any circumstances send messages or attachments whether within the CJC or outside the CJC which are:
- Abusive, including the use of foul language
 - Malicious
 - Discriminatory in any sense (e.g. sex, sexual orientation, age, race, religion, gender or disability)
 - Defamatory about any other person or organization
 - Bullying or intimidating in content
- 2.9 If you receive any such message from outside the CJC, you must delete it and must not forward it within or outside the CJC. Sending email of the type described above is likely to be treated as a disciplinary offence.
- 2.10 You should only send sensitive or confidential information when the security of the data is ensured i.e. the recipient address is a known, secure address or the email is protected.
- 2.11 Personal email accounts should not be used to send CJC information. This includes forwarding email from CJC email accounts to personal email accounts. Where there is a requirement for access to CJC emails or information away from the office this must only be via approved methods.

3. **INTERNET**

- 3.1 The CJC has put technical measures in place to prevent access to internet web sites which contain explicit, illegal or otherwise inappropriate materials. If you need to access a blocked site for the purposes of your job you must obtain express authorisation from your line manager who will, if appropriate, contact the IT Division.
- 3.2 Personal use of the CJC's Internet facilities is permitted as long as the usage is during your own time i.e. when you are clocked out and involves acceptable browsing i.e. not inappropriate websites.

3.3 It should be noted that much of the information that appears on the internet is protected by copyright. Unauthorised copying or modifying of copyright protected material, including software, breaches copyright law. Therefore, downloading software or copyright protected information is not permitted, as it may make you and/or the CJC liable to legal action.

4. **CONFIDENTIALITY**

4.1 You must not use the CJC's IT and communications systems whether alone or in conjunction with any other person to make an unauthorised disclosure or copy of sensitive, personal or business information belonging to the CJC.

4.2 The unauthorised disclosure or copying of information belonging to the CJC is likely to be treated as a disciplinary offence.

5. **MONITORING AND DATA PROTECTION**

5.1 In order to protect the interests of the CJC and to maintain the effectiveness, integrity and security of the CJC's network, the CJC has various tools in place to monitor usage of ICT systems. You should not expect that your use of the CJC's IT and communication systems is private.

5.2 The holding, processing and disclosure of personal data in electronic form is regulated by the provisions of Data Protection legislation. Personal information relating to a living individual who can be identified from that information should not be sent outside the CJC unless proper checks have been made to ensure that this will not involve any breach of that or any other legislation.

6. **SECURITY**

6.1 The login credential supplied to you to undertake your duties must never be shared with another member of staff or other person(s)

6.2 If you are provided with a portable computer, iPad, mobile phone, Blackberry, personal organiser and/or any related or similar equipment, you must ensure its security at all times. You must in particular:

- Never leave computer equipment including CDs, DVDs, flash drives, blackberry, key fob, etc. in an unattended vehicle unless the equipment is locked in the boot. If you have to leave the vehicle for any reason, this must be for the least time possible. It should be noted that often the data on the computer equipment is more valuable than the computer equipment itself.

- Never leave equipment unattended in public or unlocked where its screen can be viewed
- Always lock mobile equipment when not in use so that it cannot be used without entering your log-on details
- Keep your passwords confidential (IT systems will force you to change them regularly) and never, in any circumstances, attach the password to the device

6.3 If your computer equipment is lost or stolen you must report the incident immediately to the Monitoring Officer

6.4 You must not attempt to access any service or function of the network unless you have been granted permission.

7. **EQUIPMENT NOT PROVIDED BY THE CJC**

7.1 You must not connect, or attempt to connect, any device to the network without express CJC from the IT Division. You should be aware that the CJC may have measures in place to detect this activity.

7.2 In particular you should not attempt to connect any of the following devices to the CJC's network:

- A file/information storage device not issued by the CJC
- A mobile phone not issued by the CJC
- An MP3 Player or similar device not issued by the CJC
- A gaming device not issued by the CJC

7.3 A breach of the prohibition on connecting devices to the CJC's network is likely to be treated as a disciplinary offence.

8. **PERSONAL USE**

8.1 Personal use of the CJC's Internet/Intranet facility is permitted subject to the following rules:

- Personal Internet usage is in your own time i.e. when clocked out
- Personal Intranet usage e.g. to the classifieds section is in your own time i.e. when clocked out
- You may not subscribe to any non-job related Internet service e.g. BBC tickertape.

- You may not use the CJC's systems to transfer, store or download information and files for your personal use including (but not limited to) MP3, AVI, WMV, MPEG, etc.
- 8.2 If your personal use exceeds an acceptable level in the reasonable opinion of the CJC or you do not comply with these rules your access may be curtailed and you may be subject to disciplinary action in line with the Disciplinary Policy and procedure and which could result in dismissal for gross misconduct.
- 8.3 Personal use of CJC equipment exclusive of Internet access is not permitted unless sanctioned by the Chief Executive
- 8.4 Unauthorised individuals must not install software on CJC devices or machines.
- 8.5 CJC person identifiable or sensitive information or business data must not be stored on a device which is not owned by the CJC unless specifically authorised is granted.

9. GENERAL QUERIES

- 9.1 Any questions regarding this policy or computer security in general should be addressed to the Monitoring Officer.