C6.5 Appropriate Use of Government Computers Brigade

What I Need to Know

Computers purchased by brigades utilising public money or donated directly to the brigade are considered to be the property of the Department of Emergency Services. Because of this, government guidelines must be followed when this equipment is used by volunteers.

Key Issues/Risks:

Unauthorised access to DES information or computer systems is open to the risk of compromise or unauthorised modification.

Inappropriate use of the Internet or email by DES personnel or **volunteers** may result in litigation against, or damage to the reputation of, the DES and/or the Queensland Government.

How I do it

Responsibilities:

- All volunteers utilising DES computers must:
  - ensure that their internet, intranet and email use falls within the definition of appropriate use and not within the definition of unacceptable use as detailed in this practice statement;
  - report suspected or identified unacceptable use of the internet, or email services to their Area Director, Rural Operations;
  - use reasonable care choosing email content to be sent across the internet and to ensure it is not offensive, threatening or otherwise unacceptable;
  - ensure that any files received by email or downloaded from the internet are scanned for viruses before being used on DES systems; and
  - comply with the requirements of this practice statement and any related DES policies and practices when using internet and email services.

Appropriate use:

- Internet and email services will be used for the following purposes:
  - Conducting official DES business;
  - Education and self-development, as agreed with line management;
  - Limited personal use.
- All use of Internet and email services will be:
  - appropriate for its purpose;
  - lawful (in accordance with Australian and International laws);
  - consistent with DES policies and standards, State and Federal Government regulations and policies; and
  - able to undergo public and / or agency scrutiny.

Personal Use

- The user’s personal use access rights may be revoked at any time if that use is not in accordance with the following requirements:
  - must be consistent with the professional, legal, moral and ethical standards expected of QRFS personnel and volunteers;
  - must be infrequent and brief;

  - must not violate any Federal or State government legislation, regulation or policy, or agency policy; and
  - must not constitute "unacceptable use" as defined in this practice statement.

- QFRS reserves the right to require reimbursement of costs for excessive personal use.
- QFRS takes no responsibility regarding the transmission by Brigade members of personal information over the Internet.

Unacceptable Use

- Unacceptable use of QFRS Internet, Intranet and email services is not authorised and will attract disciplinary action. QFRS may also refer incidents of unacceptable use to the Crime and Misconduct Commission or relevant law enforcement agencies.
- Brigade members will ensure that their use of Internet, Intranet and email services is not considered unacceptable and does not contravene the requirements of this practice statement.
- Use of Internet, Intranet and email services that is unacceptable within QFRS includes the following:
  - Unlawful use, including Criminal Offences; and
  - Inappropriate use.
- The following are examples of use within these categories:

Unlawful use, including criminal offences

- Downloading, storing, distributing or communicating information on the location of child pornography
- Breach of copyright, such as unlicensed copying of a computer program
- Intercepting or attempting to steal or alter information; unlawfully accessing, altering, distributing or falsifying electronic documents or programs
- Unauthorised access to a website or other server accessible of the Internet and / or making unauthorised modifications to any public Internet site through hacking activity
- Accessing or downloading website material or files, or transmitting material, that is defamatory
- Disseminating messages without authority that may cause people to fear for their safety or the safety of others
- Intentionally intercepting, eavesdropping, recording, reading or altering another person's email messages without authorisation
- Breaches of conditions placed upon a user as part of the DES Code of Conduct or complementary Statutory Authority Code of Conduct, Public Sector Ethics Act 1994 (QLD), Public Service Act 1996 (QLD) or related State and Federal legislation and regulations.

Inappropriate Use

- Excessive personal use (refer to section on Personal Use)
- Disseminating jokes about religious practices or social customs, or attributing stereotypical behaviour to a particular group
- Accessing, downloading, storing, and distributing pornography or distributing information on the location of pornography
- Conducting private business for personal gain or profit, including, but not limited to, fee-based and subscription services
- Creation or distribution of malicious or harmful material in any form
- Attempts to obscure the origin of any message
- Downloading material under an assumed identity or otherwise disguising own user identity in any way
- Downloading or storage of files and records not directly related to an RFS member’s official duties and not representing acceptable personal use as defined in this practice statement

    - Using Departmental computers to send or receive facsimiles
    - Failure to use care when accepting and reading unsolicited mail as this could contain electronic viruses
    - Failure to undertake agency security precautions when downloading files, documents or software such as checking for viruses
    - Failure to protect the privacy of any individual by unnecessarily distributing their personal information
    - Failure to keep passwords secure
    - Disrupting other QFRS users or QFRS services or QFRS equipment through such means as, but not limited to, mass mailing or transmitting of files and documents
    - Damaging, deleting, inserting or otherwise altering information with malicious intent
    - Representing personal opinions as those of the agency, or otherwise failing to comply with agency practices concerning public statements about the government's position

Security Tools

- Accessing, downloading, and disseminating or using any program from the Internet that can be used to test the security of a system or compromise the security of a system is strictly forbidden. This includes:
    - password cracking software
    - vulnerability scanning software
    - remote access software
    - encryption software
    - spying or recording software
    - telephone dialling software.
- Installation of such tools on QFRS equipment will be viewed extremely seriously by management.

Confidentiality

- Email sent over the Internet is usually transmitted in "clear-text", meaning that it can be intercepted and read by anyone. Volunteers need to use reasonable judgement in choosing the content of email messages sent externally to DES.

DES Websites (including brigade-specific websites)

- All information should be reviewed for confidentiality and privacy requirements prior to being posted on any externally accessible QFRS web site.
- Unauthorised access and / or modification to QFRS sites are forbidden.

Licensing

- All programs downloaded from the Internet or installed on QFRS systems must be appropriately licensed.

Reference Materials

- Area Reference Manual - Business Rule: C4.2.2 Maintain Area Knowledge Resources
- Department of Emergency Services Policies
- DES Internet and Email Usage Practice Statement
- Security of DES Information and Communication Technology Statement
- Volunteer records: Information privacy