QFES

QFES Acceptable Use Policy

Version 1.1

Contents

1 Overview

1.1 Purpose

The purpose of this policy is to define and highlight those principles and actions that are considered acceptable and unacceptable when members of the QFES workforce, paid and volunteer, access Queensland Fire and Emergency Services (QFES) information assets.

This policy is in place to protect members of the QFES workforce, paid and volunteer, and QFES. Inappropriate use exposes the organisation to risks including virus attacks, compromise of network systems and services, and legal issues.

This policy is written to be consistent with the Information Security Standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013 and supports the Queensland Government Information Standard 38 Requirement that:

“Agencies must develop, implement and communicate clear and unambiguous policies and guidelines addressing the use and monitoring of ICT facilities and devices within the agency.”

1.2 Scope

This policy encompasses all of the QFES workforce, paid and volunteer, and governs the common principles behind the use of all electronic communication and information devices. It deals with authorisation, allocation, privacy and monitoring, information ownership, legal usage regulations and security.

The requirements and expectations outlined in this policy apply equally to:

- All full-time, part-time, temporary or casual QFES employees;
- State Emergency Service (SES) volunteers;
- Rural Fire Service (RFS) volunteers;
- Any other approved QFES volunteers;
- All contractors engaged by QFES;
- All third parties providing services to QFES.

In this document reference to the QFES workforce, paid and volunteer, includes all of the above categories. A volunteer is an unpaid member of SES or RFS who provides services to the community.

ICT facilities and devices include, but are not limited to:

- Desktop computers, laptops, tablets and handheld devices;
- Network accessible storage and local computer storage;
- Removable media, e.g. CDs, USB thumb drives, portable storage devices;
- Electronic networks, internet;
- Email, web mail;
- Web services;
- Printers (and other imaging equipment) and multi-function devices;
- Photocopiers;
- Fax machines;
- Telephones, including mobile telephones;

- Radios or other high frequency communication devices;
- Televisions;
- Digital or analogue recorders, including DVD and video;
- Cameras.
- Office 365.

1.3 Authority and Endorsement

This policy is published under the authority and endorsement of Deputy Commissioner Smith.

1.4 Policy Review

This policy shall be reviewed annually or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

Reviews shall incorporate:

- Assessment of opportunities for improvement of QFES's approach to information security;
- Consideration of changes to the organisational environment, business circumstances, legal conditions, or the technical environment.

Policies will be endorsed by Deputy Commissioner Smith.

1.5 Compliance and Enforcement

Non-compliance with this policy, depending on the severity and nature of the non-compliance, may result in:

- action in accordance with the Code of Conduct for QFES and/or
- withdrawal of access to QFES information systems and/or
- for illegal actions, referral to the Queensland Police Service (QPS).

1.6 Related Documents

Electronic Communications and Email Policy

1.7 Roles and Responsibilities

Role	Responsibility
Commissioner	Responsible for establishing adequate controls to comply with this policy, including authorising personnel to monitor and audit the use of electronic communication and information devices. Responsible for establishing an ongoing information security awareness campaign intended to raise members' of the QFES workforce, paid and volunteer, security awareness when using QFES's information and communication devices.
Managers and Supervisors	Responsible for advising members of the QFES workforce, paid and volunteer, and contractors of their obligations under this policy, monitoring and where necessary enforcing the policies.

Role	Responsibility
Members of the QFES workforce, paid and volunteer, contractors and third parties	Ethical and efficient in their use of electronic communication and information devices as prescribed in this general policy and other related policies.
QFES workforce, paid and volunteer	Reporting security incidents and any identified weaknesses.

2 Key Principles

Unless otherwise authorised in this policy, QFES ICT facilities and devices must be used only for official QFES business (including volunteer work), professional research and development, and limited personal use.

2.1 Approval Authorisation

Approval to use electronic communication and information devices must be obtained from the relevant line manager / QFES sponsor.

2.2 QFES Workforce Acknowledgment

Members of the QFES workforce, paid and volunteer, must acknowledge that they have read, understood and agreed to abide by policies relating to the use of electronic communication and information devices before they are assigned the privileges to use them.

2.3 Allocation

The allocation of electronic communication privileges and the access to information devices is based on the business requirements associated with a member of the QFES workforce, paid and volunteer, position or role and the allocation will be regularly reviewed to ensure continued relevance.

2.4 Ownership of Information

QFES is the legal owner of the data electronically transmitted by and stored in QFES's information services.

Documents created during the performance of a member of the QFES workforce, paid and volunteer, duties are the property of QFES. Members of the QFES workforce, paid and volunteer, cannot claim the right of intellectual ownership to such documents. Personal documents imported by a member of the QFES workforce, paid and volunteer, and used in pursuance of their duties remain the property of the QFES workforce member.

3 Acceptable Use

The primary purpose for which QFES provides members the QFES workforce, paid and volunteer, access to QFES information systems is to assist them in carrying out their duties with QFES.

QFES IT services, equipment and information are to be used for business purposes in serving the interests of the organisation, its clients and stakeholders. Their use must be ethical, lawful and appropriate, in accordance with QFES's values and policies, and with any applicable State and Commonwealth legislation and regulations.

The following section outlines expectations with respect to acceptable use of QFES's IT services, equipment and information by all members of the QFES workforce, paid and volunteer.

3.1 Information Systems

When using QFES IT systems, members of the QFES workforce, paid and volunteer, must:

- Not share use of an individual computer account;
- Protect their userid and passwords at all times;
- Be mindful of email etiquette (refer Electronic Communications and Email section);
- Log out of systems when not in use;
- Manage information in line with its classification. Refer to the Queensland Government Information Security Classification Framework;
- Report suspected breaches in compliance with QFES security policies;
- Inform management if access permissions are either:
  a. Restrictive or inhibitive to their role; or
  b. Allow access which is no longer required;

3.2 Equipment

When using QFES IT equipment, members of the QFES workforce, paid and volunteer, must:

- Protect assets inside and outside of QFES premises;
- Store equipment in a safe environment;
- Inform the Service Desk, if any malfunction or damage occurs.

3.3 Information

When using QFES information, members of the QFES workforce, paid and volunteer, must:

- Adhere to the clear desk policy when at QFES sites;
- Manage information in line with its classification. Refer to the Queensland Government Information Security Classification Framework;
- Adhere to QFES's document and records management policies and procedures;
- Exchange information only through approved channels;
- Ensure information is backed up in the appropriate repository and not stored locally;

- Consider intellectual property rights and copyright when using information and images not created or owned by QFES.

3.4 Limited Personal Use

QFES allows limited personal use of the internet and electronic communications facilities. Such use may be monitored.

3.5 Microsoft's terms of use for Office 365

The use of Office 365 requires adherence to the Microsoft's Terms of use which includes:

- Acceptable Use Policy
- Customer Portal Terms of Use
- Privacy Notice
- Trademarks.

4 Internet, Email and Social Media Use

4.1 Internet Usage

QFES permits members of the QFES workforce, paid and volunteer, to access and use the internet:

- To carry out their duties;
- To contribute to the achievement of QFES's goals and objectives;
- For initiating and furthering professional contacts; and
- For personal development.

Members of the QFES workforce, paid and volunteer, must be considerate of others, both within and outside QFES. Using the internet in a manner that may cause offence or bring QFES into disrepute is prohibited and may result in disciplinary action. Likewise, deliberate circumvention of the principles of this policy may lead to disciplinary action.

Members of the QFES workforce, paid and volunteer, must observe the following with respect to accessing the internet:

- Take all reasonable care when downloading, accessing or executing files on or from the internet services;
- The downloading (and display) of any images or material (graphical or text), which cannot be respectfully displayed in an open office area, is prohibited;
- Be extremely careful about disclosing information on the internet;
- Never disclose any user id or password associated with QFES. If accessing a site that requires a user id and password, create a separate user id and password that is completely different to your QFES user id and password;
- Carefully consider the type and nature of information requested when completing on-line application forms;
- Confidential information must not be shared on social networking sites nor are members of the QFES workforce, paid and volunteer, to post disparaging comments that may reflect poorly on QFES or its workforce, paid and volunteer, clients and stakeholders;
- All internet files including web pages, graphics and files are copyright and users must be aware that copyright restrictions apply.

4.2 Email Usage

Refer to the Electronic Communications and Email Policy for specific guidance on the usage of email and the mechanisms used for security of electronic messages within QFES.

4.3 Social Media Usage

QFES permits members of the QFES workforce, paid and volunteer, to access and use social media:

- To carry out their duties;
- To contribute to the achievement of QFES's goals and objectives;
- For initiating and furthering professional contacts;
- For communicating to wider stakeholder and community groups.

Members of the QFES workforce, paid and volunteer, must be aware of any specific agency directives and standards regarding the use of social media. Members of the QFES workforce, paid and volunteer, must also be aware that they must not publish any content on social media that may cause offence, be illegal, or bring QFES or the associated agencies into disrepute. Such a breach may result in disciplinary action.

5 Unacceptable Use

Members of the QFES workforce, paid and volunteer, must not use QFES's IT services, equipment and information for illegal, obscene, or other inappropriate activities, or in support of such activities. The following sections describe such inappropriate activity.

5.1 Copyright Infringement

Members of the QFES workforce, paid and volunteer, must not carry out activities that violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

Members of the QFES workforce, paid and volunteer, are not authorised to install or distribute "pirated" or other software products that are not appropriately licensed for use by QFES.

5.2 Misuse

Computer misuse includes, but is not limited to, the following activities whereby an individual:

- Destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of computer-based information and/or information resources;
- Interferes with the intended use of internet resources;
- Seeks to gain or gains unauthorised access to information systems;
- Seeks or gains unauthorised access to any resource or entity;
- Severely degrades or disrupts equipment or system performance;
- Attempts to read another person's protected files without proper authority;
- Reveals their account password to others or allows use of their account by others. This includes family and other household members when work is being done at home;
- Uses, or knowingly allows another to use, any computer, computer network, computer system, program or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things of value by false pretences, promises, or representations.

5.3 Offensive or Inappropriate Material

It is unacceptable for any individual to:

- Access or publish on or over the network, any information of an obscene or profane nature, or material likely to be sexually offensive to an average person or contrary to generally accepted social standards. Clear examples of such material include but are not limited to:
  a. Materials that contain sexually explicit images or descriptions;
  b. Materials that advocate illegal activity;
  c. Materials that advocate intolerance or hatred for others;
  d. Materials that are bullying or harassing in any way.
- Transmit, or cause to be transmitted, communication that may be construed as harassment or disparagement of others based on the criteria of any anti-discrimination legislation;

- Publish on or over the network any information which violates or infringes upon the rights of any other person or group, including material of an abusive nature.

5.4 System and Network Activities

The following actions are not permitted with respect to technical use of QFES information systems:

- Unauthorised copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which QFES or the end user does not have an active license;
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws;
- Knowingly introducing malicious programs into the network or server environment, e.g. viruses, worms, Trojan horses, e-mail bombs, etc.;
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to:
  a. Accessing data to which the user is not an intended recipient;
  b. Logging into a server or account that the user is not expressly authorized to access.
- For purposes of this section, "disruption" includes, but is not limited to:
  a. Network sniffing;
  b. Pinged floods;
  c. Packet spoofing;
  d. Denial of service;
  e. Forged routing information for malicious purposes.
- Port scanning or security scanning unless prior approval is obtained from the Chief Information Officer;
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty;
- Circumventing user authentication or security of any host, network or account;
- Interfering with or denying service to any user other than the employee's host, e.g. denial of service attack;
- Use of public computers such as those found in internet cafes to access QFES's systems and equipment;
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet/intranet;

5.5 Confidentiality and Privacy

Members of the QFES workforce, paid and volunteer, must not:

- Without authorisation, invade the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources;
- Share information with parties unauthorised to access QFES information;
- Provide information about, or lists of, members of the QFES workforce, paid and volunteer, to parties outside of QFES;
- Transmit cardholder data in clear text via emails, instant messaging or social media.

5.6 Inappropriate Behaviour

Inappropriate behaviour includes, but is not limited to the following actions:

- Participates in gambling activities such as may be provided by casino and internet-based gaming sites;
- Misrepresents him/herself or QFES;
- Makes fraudulent offers of products, items, or services originating from any QFES account;
- Makes statements about warranty, expressly or implied, unless it is a part of normal job duties;
- Operates a business using QFES resources;
- Violates any laws pertaining to the unauthorised use of computing resources or networks;
- Violates any State, Commonwealth, or International laws.

6 Monitoring and Privacy

QFES may choose to record access and usage logs for QFES ICT services. Access to these log files will be restricted to persons designated to perform regular and/or ad-hoc reporting in relation to those files.

Notwithstanding that emails may contain personal information, confidential information or material in which third parties own or claim copyright, QFES may access, review, monitor, and disclose the contents of all messages created, sent or received using QFES ICT services (whether solely or in part) for the purpose of monitoring compliance with this policy or compliance with any terms and conditions of employment or engagement.

All reasonable care is taken to protect members' of the QFES workforce, paid and volunteer, privacy. However, the content of personal electronic communications, documents and data may be inspected with the authorisation of a Chief Information Officer where a valid business reason exists.

7 Document Control

Author	Greg Ensbey
Approver	Deputy Commissioner Smith
Issue Date	18 August 2016
Review Date	18 August 2017
Version	1.1
Distribution	QFES workforce, paid and volunteer
Security Classification	PUBLIC DOMAIN

Date	Version	Description of Modification	Modified By
6 July 2016	0.1	Initial draft based on the PSBA policies.	Greg Ensbey
18 August 2016	1.0	Approved by Deputy Commissioner Smith	Greg Ensbey
28 November 2016	1.1	Proposed update of terminology.	Natalie Pflaum
8 December 2016	1.1	Approved by Deputy Commissioner Smith	Natalie Pflaum