
# QFES

# Electronic Communications & E-mail Policy

# Contents

# 1 Framework

## 1.1 Purpose

The Electronic Communications & Email Policy establishes the mechanisms used for security of electronic messages within the Queensland Fire and Emergency Services (QFES).

## 1.2 Objectives

This policy seeks to ensure that QFES information assets are not compromised through electronic messaging systems.

## 1.3 Scope

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

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

In this document reference to staff or personnel includes all of the above categories of staff and personnel. A volunteer is an unpaid member of SES or RFSQ who provides services to the community.

## 1.4 Authority and Endorsement

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

## 1.5 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 the ICT Strategy and Renewal Committee and approved by the Chief Executive Officer.

## 1.6 Compliance and Enforcement

Non-compliance with this policy, depending on the severity and nature of the non-compliance, may result in the department taking action in accordance with the Code of Conduct for the Queensland Public Service.

# 2 Key Principles

## 2.1 Privacy

QFES is mindful of the guidelines of the Australian Privacy Principles, and that the content of e-mail messages is generally regarded as private. However, QFES reserves the right to access, review, monitor and disclose the contents of all messages created, sent or received using its e-mail environment. This is in accordance with QFES's Information Security Policy.

The contents of e-mail messages may be monitored, captured and referenced without notifying either the recipient or sender.

## 2.2 Ownership

All e-mail messages that are created, sent or received using any of the following mechanisms are considered the property of QFES:

- The QFES e-mail service;
- QFES mailboxes within the e-mail system; and
- Any other messaging service that may be introduced;

This includes the contents of any such message.

## 2.3 Roles and Responsibilities

| Role | Responsibility |
|---|---|
| Commissioner | The provision and implementation of assets, supporting systems, applications and processes that give effect to this policy.<br>The establishment and maintenance of monitoring and compliance systems and processes to ensure that the supporting mechanisms are functioning effectively. |
| Managers & supervisors | The proper induction of new personnel, including non-permanent personnel, and to ensure that all personnel in their area are made aware of this policy and the consequences of breaching it. |
| Employees, contractors and third parties | Responsible for compliance with this policy, and any supporting policies, standards and procedures. |
| All personnel | Reporting security incidents and any identified weaknesses. |

# 3 Use and Etiquette

## 3.1 Acceptable Use

Users of QFES e-mail systems must ensure that all material made available, in any form whatsoever, appropriately represents QFES.

E-mail is provided to QFES personnel for obtaining and sending information, however:

- All users of e-mail must use their access with respect and courtesy for others and in a responsible and professional manner;
- The e-mail is provided for work-related activities and the use of e-mail for private use must be minimal;
- Operational e-mails must not be forwarded to personal e-mail addresses by either auto-forwarding or manual means unless approved by a manager or supervisor;
- Non-work related e-mail addresses and phone numbers must not be included in work related correspondence;
- Examples of acceptable use are:
    - Work-related activities;
    - Work-related professional associations;
    - Research and development;
    - Work related issues in their field of knowledge.

## 3.2 Unacceptable Use

The e-mail system is not to be used as a facility for storing or distributing information or material that falls into any of the following categories:

- Spamming (bulk broadcasting of promotional material) is not an accepted e-mail practice. Refer to the Australian Spam Act 2003;
- Offensive material such as inappropriate humour and graphics are not to be sent by e-mail. If any message of an unacceptable nature is received, then the recipient should not delete the message, but should notify the Service Desk, who will take appropriate action;
- Harassment or abuse of any kind;
- In a manner that degrades or disrupts equipment or system performance;
- Is offensive or sexually explicit;
- Contains anything that may cause or constitute sexual/racial harassment, bullying, or disparagement of others based on their race, national origin, marital status, sex, sexual orientation, age, disability, religious or political beliefs;
- Solicits, promotes or advertises any organisation, product or service;
- Financial gain including any services to be used for any personal business or commercial activity; Solicitation for other users is also not permitted, along with the distribution of advertising material;
- Promotes political lobbying;
- Participates in gambling activities, such as may be provided by, but not limited to, casino-related sites and pyramid schemes;
- Relates to facilitating the purchase of illegal drugs or pornographic material or activities;

- Contains chain letters;
- Violates any State or Commonwealth laws;
- Devises or executes a virus or Trojan program, hoaxes or practical jokes;
- Contains passwords;
- Conceals or misrepresents the identity of the sender; and
- Suggests it has QFES endorsement or a level of approval that it does not have.

Personnel must not attempt to gain access to mailboxes other than those they are authorised to use.

QFES reserves the right to take disciplinary action when a staff member is sending excessive or improper electronic mail.

### 3.3 Responsible Use

- E-mails are official records and should be filed for records management purposes in the same way as minutes and letters in accordance with the Public Records Act 2002. Any filing questions are to be referred to your line manager;
- E-mails are not necessarily delivered or read by the recipient immediately, so other forms of communication should be considered where the matter is urgent;
- Reasonable care should be taken when opening attachments received with e-mails. Virus protection measures are in place on the network, however, it is the responsibility of all personnel to take reasonable care when downloading, accessing or executing files from e-mails. If there is a suspicion that a file may have a virus associated with it, the Service Desk should be contacted immediately;
- E-mails are suitable to be used for any official business purpose;
- E-mails are to be recognised as legal documents that have the same legal implications as ‘hand written’ mail.

### 3.4 Etiquette

- E-mail should not be considered the primary communication vehicle;
- Receipt of e-mails should be regularly checked, similar to how often you would check your voice-mail or in-tray;
- If unable to answer the e-mail immediately, receipt of the e-mail should be acknowledged with an indication as to when you will be able to respond (as you would for a telephone message);
- Judgment should be used when forwarding e-mails that you have received to ensure you are not breaching the confidence of the sender or of QFES;
- QFES business emails are at times highly sensitive and confidential. Messages to and from QFES recipients are sent on the understanding that the system is secure and messages are maintained within the QFES context;
- Automatic forwarding of e-mail to third party mail boxes (e.g. Hotmail, gmail) is not allowed unless approved by a manager or supervisor;
- The use of any quoted information in an e-mail must be acknowledged;.
- Consideration should be given to not sending large attachments with e-mails as it may have an adverse implication on the recipient’s capacity to access the e-mail due to storage requirements;.
- Punctuation and spelling standards should be maintained as if sending a letter;

- Copyright standards must always be complied with.  If you are unsure of the appropriate standards, advice must be sought;.
- E-mails should be prepared in a professional manner (no matter how informal it may seem, it is a ‘written’ business communication and should be treated like a minute or letter), being polite, courteous, discreet and avoiding gossip at all times;
- E-mails are a form of written communication and judgment should be used in determining when it is appropriate to use an e-mail;
- E-mail messages must include a QFES standard signature at the end of each message.

# 4 Policy Statements

## 4.1 Security and Confidentiality

Users of e-mail should be aware that e-mail is not considered a secure form of communication and that system administrators can potentially view e-mail during the normal course of their work.

E-mails should therefore be considered as insecure and unreliable unless the message has been encrypted and digitally signed.

When deciding what information is to be included in an e-mail, consideration should be given to the fact that it may be forwarded to another party without your knowledge.

All users of the e-mail systems are responsible and accountable for e-mail sent under their identity.

### 4.1.1 Baselines

- Attachments to e-mails must conform to the processes outlined in the Information Labelling and Handling procedure.

## 4.2 Personal Use

E-mail may be used for personal use provided that:

- The messages do not overly use resources and do not impact the performance or operation of the equipment;
- They do not interfere with a person's work performance;
- It is professional, legal and consistent with the Code of Conduct for the Queensland Public Service, and QFES, information security policies and procedures.

The use of e-mails for personal use must be accepted as a privilege, not a right, and used with discretion.

### 4.2.1 Baselines

- Any personal files and documents created, accessed, sent and/or received via QFES information systems are subject to open records requests and may be accessed in accordance with QFES's information security policies, the Information Privacy Act 2009 and the Right to Information Act 2009;
- An employee's personal use access rights may be revoked at any time at the discretion of the employee's manager should use be deemed to be excessive or interfering with the employee's performance of their duties.

## 4.3 Mailbox Management

Each user in QFES is provided with a mailbox and a storage quota.

Personnel using an unacceptable amount of storage will receive notification from the Service Desk advising them that their mailbox storage is excessive and, as a consequence, they will be unable to send e-mail until the content of their mailbox is reduced below their quota, i.e. unwanted e-mail is deleted.

### 4.3.1 Baselines

- The content and maintenance of an electronic mailbox is the responsibility of the user;

- Personnel should regularly review the content of their mailbox to delete or archive out of date or irrelevant e-mail communications and update personal distribution lists;
- E-mail users who have left QFES will have their mailbox forwarded to a suitable recipient for a period of time and then deleted, in line with current exit procedures.

## 4.4 Records Management

The e-mail system is in no way perceived to be a paperless office system. E-mail should be considered as an electronic vehicle by which communication is passed to the recipient and treated no differently to other correspondence.

### 4.4.1 Baselines

- E-mails and attachments should be kept and filed in accordance with normal administrative practice;
- To achieve this, hard copies of e-mails and attachments may need to be filed with other relevant written communications.

## 4.5 E-mail Signatures

E-mail messages should include a signature block attached to the end of each message. This signature block will be provided by the Service Desk. It will include a disclaimer.

This requirement is necessary to ensure compliance with the Australian Spam Act 2003 in order to provide the receiver with the ability to contact the e-mail sender.

### 4.5.1 Baselines

- All e-mail messages should include a signature field at the bottom of each message that is compliant with the QFES standard.

## 4.6 Unsolicited E-mail

Personnel must take care not to send unsolicited e-mail that may breach legislative requirements. Spam is defined as “unsolicited commercial electronic messaging”.

Personnel found to be breaching legislation will be subject to disciplinary action.

### 4.6.1 Baselines

- Prior to sending unsolicited e-mail, personnel should review relevant legislation;
- Prior to sending unsolicited e-mail, personnel should ensure they have ‘consent’ to send the mail as defined in the relevant legislation. Consent is generally defined as having some sort of existing relationship with the receiver.

## 4.7 Distribution Lists

Distribution of e-mail to large numbers of users both inside and outside of QFES is prohibited unless specifically approved. This sort of e-mail can be considered spam and care must be taken to ensure that breach of the relevant legislation does not occur.

### 4.7.1 Baselines

- All personnel must obtain approval prior to sending of bulk e-mail;
- Prior to sending unsolicited e-mail users should review the relevant legislation.

## 4.8 Junk Mail and Mailing Lists

Bulk e-mail sent to one or more mailboxes can overload the e-mail systems, causing downtime and delays in sending and receiving e-mail for all e-mail system users.

Personnel should avoid subscribing to mailing lists unless they are required for business purposes. A mailing list is similar to a junk mail list and can result in a user being constantly bombarded with electronic mail. Apart from wasting productive time, junk mail may also saturate the communications links and cause impact on the ability of personnel to perform normal day to day tasks.

### 4.8.1 Baselines

- Personnel should not subscribe to non-work related mailing lists;
- Personnel should not click 'unsubscribe' if unsolicited e-mail is received.

## 4.9 Phishing

"Phishing" is a term coined for the activity of gaining information through social engineering or by relying on the trust or good nature of people. The most common form of phishing is an e-mail purporting to be from a legitimate source such as an administrator, a well-known business or, more commonly, a bank. The e-mail will ask the user to click on a link to perform some action. Commonly the action is to logon to re-enable your account or prevent some sort of unwanted action from occurring such as an account lockout.

Personnel should be aware of such e-mails and report all suspicious e-mail to the Service Desk, particularly e-mails asking for passwords or personal information.

### 4.9.1 Baselines

- Personnel should refrain from clicking on embedded URLs (web links) in e-mails. Instead they should open a new browser window and manually type the known link. For instance, if you receive an e-mail from Westpac asking to logon, open a browser window and type the known Westpac link, not the link suggested in the e-mail message;
- Report suspicious e-mail to the Service Desk;
- Take care not to include personal information in e-mail messages.

## 4.10 Monitoring

The compliance of personnel with this policy will be reviewed periodically by relevant information security personnel.

To prevent loss, data is regularly backed up by technical personnel. The process results in the copying of e-mails onto storage media that may be retained in unidentified locations. Network administrators during the course of their work may see e-mails and are obligated to report policy violations.

## 4.11 Audit

QFES is mindful of the requirements of the various privacy regulations in the jurisdictions in which it operates and, in addition, that some information is generally regarded as private. However, QFES has the right to access, review, monitor and disclose information to ensure that:

- Information processing systems are used appropriately;
- Information assets are protected; and
- Legal responsibilities are met.

Management reserves the right to monitor, inspect and/or search at any time all of QFES information systems to confirm compliance with internal policies, as well as applicable laws and regulations and to monitor staff safety subject to applicable laws and regulations.

Staff should have no presumption or expectation of privacy in their use of QFES networks, systems and facilities.

Requests to access employee e-mail and or network files for reasons related to suspected misuse must be directed to Information Security Operation group in the first instance who will then liaise with other relevant personnel as required. Requests will only be met if, in the view of the Chief Information Officer, accessing records is necessary to investigate a claim or confirm a reasonable suspicion.

### 4.12 Virus Scanning

Attachments contained within e-mails or e-mails detected as virus infected will either be repaired or deleted with a notification forwarded to the intended recipient and/or sender as required.

## 4.13 Filtering

QFES may implement and/or maintain e-mail filtering software to enable content monitoring and, in selected circumstances, content blocking to:

- Provide early protection against new viruses;
- Prevent unauthorised or inappropriate disclosure of confidential information to internet e-mail addresses; and
- Prevent offensive or sexually explicit material being propagated.

# 5 Instant Messaging and Peer-to-Peer Software

QFES may choose to use instant messaging (IM) technology to reduce operational costs and improve contact and communications capability within the organisation.

## 5.1 Instant Messaging

Popular instant messaging tools such as Skype and Facebook Messenger are not prohibited for personal or business use.

There is a requirement that the most current version of the IM software is installed to protect against bugs and potential security issues, and that anti-virus software must be installed and operational at all times.

## 5.2 Peer-to-Peer

The use of peer-to-peer (P2P) software such as Bit torrent, FlashGet, Gnutella, and any other similar software is strictly prohibited in QFES. There are no exceptions to this rule.

Personnel found to have installed or to be using peer-to-peer software will be subject to disciplinary action.

### 5.2.1 Baselines

a) You may not, under any circumstance, install any peer-to-peer file-sharing software on any computer owned by QFES;
b) You may not connect any personally owned computer to a QFES network if it has peer-to-peer file-sharing software on it.

# 6 Voice Communications

## 6.1 Security and Confidentiality

QFES staff communicate with clients and other various stakeholders via both landlines and mobile phones.

Personnel should be aware of the risks of wire-tapping and monitoring of both communications means, and be particularly aware of using mobile phones in public places where the risk of eavesdroppers is high.

### 6.1.1 Baselines

- Personnel should not discuss sensitive matters on mobile phones in public places including cafés, taxis, airports, meetings etc.
- Personnel should be aware that communications may be monitored, either knowingly or unknowingly, on third party sites and refrain from discussing sensitive matters.

## 6.2 Etiquette

- Personnel should also be aware of the 'annoyance' of mobile phones to other people, particularly when meeting or communicating with clients;
- During meetings, phones must be switched to silent mode. You should not answer or make calls when in meetings;
- Landline calls must be answered professionally;
- When calling a third party, always announce yourself. Do not make the assumption that they will know who you are;
- If you take a message for another person, send that person an e-mail message containing:
    - Name of caller
    - Number of caller
    - Brief details of the call

# 7 Fax

## 7.1 Security and Confidentiality

Users of fax equipment should be aware that fax transmissions are not considered a secure form of communication and that fax messages can be easily misplaced or viewed inappropriately at the recipient address.

Fax transmission should therefore be considered as insecure and unreliable.

When deciding what information is to be included in a fax, consideration should be given to the fact that it may be forwarded to another party without your knowledge and that unauthorised persons may view the fax at the recipient address.

### 7.1.1 Baselines

- All outgoing fax messages must include a standard QFES fax coversheet;
- When sending information that may be sensitive, refer to the Information Labelling and Handling procedure for guidance;
- When receiving sensitive information, liaise with the sender and ensure you are on hand to receive and acknowledge receipt of the fax.

## 7.2 Etiquette and Handling

When information is transmitted via a QFES fax, ensure that there are reasonable security measures for the information being sent or received during the transmission of a fax.

When using the fax to transmit or receive confidential or personal information, you must consider the following security precautions depending on the sensitivity of the documents:

- Determine if the recipient's fax machine is in a secure area and that there is a means of securing documents containing confidential or personal information upon its arrival;
- If the information being transmitted is particularly sensitive, you may need to contact the recipient before transmission to ensure that he/she is available to receive the material immediately;
- For sensitive material, it is recommended to phone the recipient to confirm receipt of the fax or request the recipient to phone you when he/she receives the information;
- If this is not possible, check the fax transmission report to ensure a correct transmission and this may enable immediate action if information was not transmitted correctly;
- Ensure that the document being faxed has a cover sheet with a confidentiality statement. The confidentiality statement is in addition to other QFES information on the cover sheet such as the name, phone and fax number of the sender and the number of pages being sent;
- Upon receipt of a fax at QFES, place the faxed pages in the staff in-tray of the addressed staff recipient.

# 8 Document Control

| | |
|---|---|
| **Author** | Greg Ensbey |
| **Approver** | Deputy Commissioner Smith |
| **Issue Date** | 18 August 2016 |
| **Review Date** | 18 August 2017 |
| **Version** | 1.0 |
| **Doc Id** | Queensland Fire and Emergency Services |
| **Distribution** | All internal staff |
| **Description** | Internal procedure only. |
| **Security Classification** | PUBLIC DOMAIN |

| Date | Version | Description of Modification | Modified By |
|---|---|---|---|
| 6 July 2016 | 0.1 | Initial draft based on the PSBA policy | Greg Ensbey |
| 18 July 2016 | 1.0 | Approved by Deputy Commissioner Smith | Greg Ensbey |