Government of South Australia

South Australian Fire and Emergency Services Commission

Internet and Email Use

POLICY

1 PUBLIC SECTOR VALUES

The *South Australian Public Sector Values and Behavioural Framework* and the *Code of Ethics for the South Australian Public Sector* (the Code of Ethics) describe the values and behaviours expected of all public sector employees, namely:

- Service – proudly serve the community and Government of South Australia
- Professionalism – strive for excellence
- Trust – we have confidence in the ability of others
- Respect – we value every individual
- Collaboration & Engagement – we create solutions together
- Honesty & Integrity – we act truthfully, consistently and fairly
- Courage & Tenacity – we never give up
- Sustainability – we work to get the best results for current and future generations of South Australians

Volunteers are similarly required to uphold the principles of good conduct and standards of behaviour expected of public sector employees whilst performing their volunteering duties and functions; to observe similar ethical, policy and/or legislative requirements as employees.

This policy is guided by one or more of these public sector values and behaviours, and supports the emergency services sector in achieving our vision of *"A trusted fire and emergency services sector building safer and more resilient communities".*

2 PURPOSE

This policy defines the obligations of Emergency Services Sector (ESS) employees, contractors and volunteers when using internet and email facilities. Its purpose is to promote the responsible use of ESS and SA Government internet and email facilities and to ensure the sector complies with the *SA Government Cyber Security Framework (SACSF).*

The objectives of this policy are to ensure:

- that the sector and the SA Government are protected from illegal, unethical and inappropriate use of SA Government internet and email facilities.
- Appropriate use of SA Government internet and email facilities.

3 SCOPE

This policy applies to all employees, volunteers and contracted staff who access the ESS network for access to the internet and email including remote access.

Compliance with this policy is a condition of access to the ESS network and internet facilities.

4 DEFINITIONS AND ACRONYMS

CFS	South Australian Country Fire Service.
ESS	Emergency services sector, comprising: South Australian Fire & Emergency Services Commission, South Australian Country Fire Service (CFS), South Australian Metropolitan Fire Service (MFS), and South Australian State Emergency Service (SES).
ESS Executive	Comprises: Chief Executive SAFECOM; Chief Officer MFS; Chief Officer CFS; Chief Officer SES.
Manager	Any role and occupant of that role with employee responsibilities. May include Directors, Managers, Branch Managers and Regional Commanders.
Employee	Employees as defined in the: *Fire and Emergency Services Act 2005*, *Public Sector Act 2009*, and *Return to Work Act 2014*.
MFS	South Australian Metropolitan Fire Service.
SAFECOM	South Australian Fire and Emergency Services Commission.
SES	South Australian State Emergency Service.
Chain letter	An email that urges you to forward copies to other people.
Download	The transfer of any material from the internet to your computer. When a webpage is accessed the document along with associated graphics are downloaded from a web server to your computer.
Excessive non-business use	Non-business use which: • Occurs during normal working hours (excluding lunch or other official breaks) • Adversely affects, or could reasonably be expected to adversely affect the performance of an employee's duties • Incurs significant download costs.
SACSF	*SA Government Cyber Security Framework (SACSF)*.
Malware	Malicious computer software that interferes with normal computer functions or sends personal data about the user to unauthorised parties over the internet.
Non-business use	Use of internet or email facilities for purposes other than conducting agency business.
Spam	Unsolicited commercial email, also known as junk email
Unusual use	Patterns of use that may indicate inappropriate or excessive non-business use.
Volunteer	A registered member of CFS or SES who carries out community work within the emergency services sector on a voluntary basis.

5 POLICY POSITION

5.1 Policy and legislative context

The use of email and the access and use of information on the internet are subject to State and Federal legislation and SA Government direction. Non-compliance with the intent and conditions prescribed within these Acts can result in penalties against the user and/or the ESS.

Users of sector internet and email facilities must have particular regard to the:

- *Equal Opportunity Act 1984*
- *Racial Discrimination Act 1975*, which has wider provisions and applies to State employees and contractors alike
- *Electronic Transactions Act 2000*
- *Code of Ethics for the South Australian Public Sector*
- *State Records Act 1997* and *SA Government Adequate Records Management Standards* in relation to the capture of official records

- The list of the additional applicable laws, instructions and guidelines contained in this policy at section 9. Related documents.

5.2 Appropriate use

5.2.1 Appropriate non-business use

Internet and email facilities are provided for ESS business use however limited non-business use in personal time is also acceptable. Such use must have regard to employee obligations to discharge their duties conscientiously and to obey applicable laws, and must be consistent with this policy.

5.2.2 Internet and email code of conduct

The following code of conduct must be adhered to in relation to internet and email use:

- Deliberate or systematic inappropriate or excessive non-business use of SA Government internet and email facilities is not permitted.
- Accessing internet sites that contain the following content is unacceptable:
  - Sexually explicit material;
  - Hate speech or offensive material;
  - Material regarding illicit drugs, violence, criminal skills and/or illegal activities; and
  - Material that seeks to defame, discriminate or harass.

Non-compliance with this policy may be subject to disciplinary action.

Further direction on appropriate use of internet and email facilities is provided in sections 5.2.3 and 5.2.4 of this policy.

5.2.3 Internet Use

ESS employees are expected to use internet services responsibly with the normal standards of professional courtesy and conduct.

The ESS acknowledges that inappropriate sites can be accessed inadvertently. Should this situation eventuate users should close the relevant site(s) immediately. Deliberate, prolonged or systematic access to inappropriate material however, will not be tolerated.

The ESS reserves the right to block sites that are deemed inappropriate. Such sites may include, but are not limited to gambling, pornographic or malware content.

Inappropriate use of the internet

Internet services shall not be used for unlawful activities; commercial purposes not approved by the ESS; or for personal use that otherwise violates ESS or SA Government policies or guidelines.

Internet services shall not be used for purposes that could cause:

- Excessive downloading of files;
- File sharing by implementing any peer to peer file sharing service; or
- Scanning for, or trying to exploit vulnerabilities of the ESS network or any other network.

5.2.4 Email use

- Email should only be used for appropriate business reasons or to allow ESS employees to create efficiencies within their work time.
- Email messages are considered to be official records when they are made or received in the conducted of ESS business and must be managed in accordance with the *State Records Act 1997.*

- Email messages may also be discoverable under the *Freedom of Information Act 1991*, and are subject to the provisions of the *Evidence Act 1929* and *Electronic Transactions Act 2000*.
- Information released via email must adhere to the standards expected for all ESS external communication and should be courteous, professional and use appropriate expression and language.
- The transmission of obscene, defamatory or harassing email is prohibited, as is the distribution of email chain letters, spam or any other material which could be considered annoying or offensive.
- Email accounts remain the property of the ESS. Individual emails and email accounts may be monitored or accessed in order to ensure the appropriate use of ESS resources or for any other reason deemed necessary by the relevant Chief Executive / Chief Officer.
- Highly confidential or sensitive information should not be transmitted via email.
- Email must not be configured to automatically forward to external email addresses.
- Email services shall not be used for unlawful activities; commercial purposes not approved by the ESS; or defamation, political lobbying or personal use that violates other ESS policies or guidelines.
- Wherever possible, ESS business email correspondence should be conducted using ESS provided email accounts.
- Security controls will be enforced on mobile devices including private devices used to access SA Government information. Including device encryption, device password/PIN enforced, and remote wipe functionality is enabled on all mobile devices used for work.
- SA Government email can only be accessed via the Outlook App (not the native email client).
- Outlook Web Access and Office 365 applications can only be accessed via Microsoft Edge as the approved browser.

Automatic email signature

ESS business emails sent outside the agency must include a signature block that appropriately identifies the sender.

5.3 Monitoring

Use of the ESS internet and email facilities is logged and may be monitored by authorised persons. Regular internet usage reports can be provided to managers which highlight downloads and most commonly accessed sites as possible indicators of inappropriate or excessive non-business use.

Where unusual use patterns or other concerns suggest that further investigation may be required, additional reports can be supplied to authorised persons identifying times of use and sites visited by specific users.

In addition, SAFECOM IT may initiate investigations based on certain triggers, including high level use of non-business sites and any access of inappropriate sites.

Managers are responsible for addressing identified unusual use with the relevant employees.

5.4 Security

Users must immediately notify the SAFECOM Helpdesk of the loss or theft of a login name or password, or where they have reason to believe that someone has obtained unauthorised access to SAFECOM IT assets, including systems or to an ESS network user account.

5.5 Records and information management requirements

Email messages created or received by ESS employees that provide evidence of ESS business are records and, as such, are governed by the same range of policy principles and guidelines that affect all other ESS records and information.

6 ROLES AND RESPONSIBILITIES

Role	Responsibility
ESS Executive	Approve the policy and any associated guideline(s) as relevant.
ESS Executive	Disseminate and implement the policy and any associated guideline(s) as relevant within own agency.
Manager IMS	Review the policy and any associated guideline(s).
Manager IMS	Interpretation and advice.
Managers	Implementation of policy and any associated guideline(s) as relevant.
Employees	Complying with this policy and any associated guideline(s) as relevant.

7 REVIEW

This policy will be reviewed in two years unless significant changes are required before that time.

8 DOCUMENT HISTORY

Date	Version	Description
December 2016	1	Policy created
August 2022	1.1	Policy updated

9 RELATED DOCUMENTS

The following ESS and SA Government policies and Commonwealth and State legislation are relevant and should be read in consultation with this policy:

SA Government and ESS policies

- *Code of Ethics for the South Australian Public Sector*
- *South Australian Public Sector Values and Behaviours Framework*
- *SA Government Adequate Records Management Standards*
- *SA Government Cyber Security Framework (SACSF)*
- ESS Records Management Policy
- ESS Information Security Classification Policy and Procedure
- ESS User Identity and Password Policy

Legislation

South Australian Consolidated Acts:

- *Fire and Emergency Services Act 2005* and *Regulations*
- *Criminal Law Consolidation Act 1935*
- *Electronic Transactions Act 2000*
- *Equal Opportunity Act 1984*

- *Evidence Act 1929*
- *Freedom of Information Act 1991*
- *Public Sector Act 2009*
- *Public Sector (Honesty and Accountability) Act 1995* and *Regulations*
- *State Records Act 1997*
- *Summary Offences Act 1953*
- *Whistleblowers Protection Act 1993*
- *Work Health and Safety Act 2012*

Commonwealth Consolidated Acts:

- *Copyright Act 1968*
- *Disability Discrimination Act 1992*
- *Freedom of Information Act 1982*
- *Privacy Act 1988*
- *Racial Discrimination Act 1975*
- *Sex Discrimination Act 1984*
- *Spam Act 2003*

10 APPROVAL

Julia Waddington-Powell
Chief Executive
SAFECOM

24 / 11 / 2022

Michael Morgan
Chief Officer
SA Metropolitan Fire Service

21 / 11 / 2022

Brett Loughlin
Chief Officer
SA Country Fire Service

22 / 11/ 2022

Chris Beattie

Chris Beattie
Chief Officer
SA State Emergency Service

16 / 11 / 2022