Doc 1

GENERAL ORDER 8450
INFORMATION TECHNOLOGY MANAGEMENT

General Order title	General Order 8450, **Information technology management, Email**
Date of issue	11 January 2023
Date of operation	30 December 2022
Review date	November 2025
Review responsibility	Customer Service Branch, Information Systems and Technology Service
Replaces	Previous General Order 8450, **Information technology management, Email**
PCO reference	2015/2209
Gazette reference	SAPG 7/23
Enquiries to	Information Systems and Technology Service Telephone 732 23333
Corporate Policy Sponsor	Executive Director, Information Systems and Technology Service

General Orders provide an employee with instructions to ensure organisational standards are maintained consistent with SAPOL's vision. To this end, General Orders are issued to assist an employee to effectively and efficiently perform their duties. It is important that an employee constantly bears in mind that the extent of their compliance with General Orders may have legal consequences.

Most orders, as is indicated by the form in which they are expressed, are mandatory and must be followed. However, not all situations encountered by an employee can be managed without some form of guidance and so some of these orders are prepared as guidelines, which should be applied using reason. An appendix to a General Order will be regarded as part of the General Order to which it relates. At all times an employee is expected to act ethically and with integrity and to be in a position to explain their actions. Deviation from these orders without justification may attract disciplinary action.

To ensure best practice an employee should be conversant with the contents of General Orders.

The contents of General Orders must not be divulged to any person not officially connected with SAPOL. Requests for General Orders will be managed as follows:

- Civil subpoena and disclosure requests—contact the Information Release Unit.
- Criminal subpoena and disclosure requests—refer to General Order, **Disclosure compliance and subpoena management**.
- Freedom of information requests—contact the Freedom of Information Unit.
- Any other requests (including requests by employees)—refer to instructions provided within General Order, **Corporate policy framework**, **5. GENERAL ORDER REQUESTS/RELEASE**.

CONTENTS

1. GENERAL ORDER STATEMENT 4

General email system 4

Secure email system 4

Scope 4

2. DEFINITIONS 4

3. ROLES AND RESPONSIBILITIES 6

All employees 6

Secure email system users 6

4. PROCEDURES 7

Allocation of email accounts 7

General email accounts 7

Secure email accounts 7

Removal of email accounts 7

General email accounts 7

Secure email accounts 7

Group email 7

Emails to DL:SAPOL All Staff 8

Whole of government emails (alert, notification and information messages) 8

User agreement 8

Monitoring 9

Management of emails as corporate records 9

General use of email system 9

Email security 10

Reasonable private use 10

Signature block 11

Disclaimer 11

5. REFERENCES 11

6. FURTHER ENQUIRIES 12

7. DOCUMENT HISTORY SINCE 25/03/09 12

1. GENERAL ORDER STATEMENT

This General Order applies to both the general email system and the Australian Law Enforcement Intelligence Network (ALEIN) secure email system.

All electronic mail addresses, accounts, messages and attachments stored in either email system are the property of SAPOL.

Employees are accountable for adhering to records management responsibilities when using email.

General email system

The general email system is provided by SAPOL to enable information, including attachments, to be transferred from one person to another (or others) for business-related purposes, and to enable business-related meetings, workshops, work commitments, et cetera to be scheduled.

Use of the general email system for other than SAPOL business-related use is only permitted as allowed by this General Order. An employee will be held accountable for their use and may be personally liable for any misuse.

Secure email system

The secure email system is provided by SAPOL to enable the exchange of *Protected* (and higher classification) information between users for business-related purposes. Use of the secure email system for other than business-related purposes is not approved. Email sent for other than a business-related purpose should be exchanged using the general email system, and in accordance with this General Order.

The secure email system is intended for the secure exchange of classified material within the scope of an employee's duties.

This General Order provides guidance on the appropriate use of the system in order to reduce the risk of inappropriate information disclosure or data breach within SAPOL. The appropriate handling of classified material is required under the South Australian Government's Cyber Security Framework (SACSF), the Australian Government's Information Security Manual (ISM), and the Protective Security Policy Framework (PSPF).

Scope

This General Order applies to each user of:

- the general email system; and/or
- the secure email system.

2. DEFINITIONS

Employee—includes employees employed under the *Police Act 1998*, *Public Sector Act 2009*, weekly paid, contractors, volunteers, managed service providers and third parties.

Reasonable private use—the following breakdown of the definition must be read in conjunction with **4. PROCEDURES, Reasonable private use** further in this General Order:

- 'Reasonable' is what could be tolerated as sensible and limited use of the general email system and where that use conforms to the following:
  - does not adversely impact on the user's SAPOL work requirements
  - does not adversely impact on the SAPOL/South Australian Government email system networks
  - does not include large, or offensive or inappropriate streaming sound files, video clips, photos, content, et cetera attached to, or embedded in, the email
  - does not contravene any part of this General Order, or commonwealth or state laws
  - does not contravene any part of General Order, **Secondary employment** and General Order, **Secondary employment (Public Sector Act, Protective Security Act and weekly paid)**.
- 'Private use'—refers to activities, communications, et cetera that does not relate to SAPOL business, notwithstanding that it may occur on SAPOL premises. Private use is not to contravene any aspects of the respective Codes of Conduct for employees, including those located within the:
  - *Police Complaints and Discipline Act 2016* and Police Complaints and Discipline Regulations 2017
  - *Public Sector Act 2009*—Part 3 Public sector principles and practices.

Record—defined by section 3 of the *State Records Act 1997* as written, graphic or pictorial matter, or a disk, tape, film, or other object that contains information or from which information may be reproduced (with or without the aid of another object or device). Given this definition, email messages are records—refer to **4. PROCEDURES, Management of emails as corporate records** further in this General Order.

Official record—defined by section 3 of the *State Records Act 1997* as information created, received and maintained as evidence and information by an organisation (agency) or person, in pursuance of legal obligations or in the transaction of business.

Email messages are official records, as defined by the *State Records Act 1997* when they are made or received in the conduct of agency business. Such business may be the provision of services, delivery of programs, development of policies, making of decisions, performance of agency functions and other similar types of transactions.

Misuse—includes storing and/or transmitting unauthorised material—specifically material relating to, but not limited to:

- death
- disfigurement
- cruelty
- violence
- pornography
- paedophilia

- material which contravenes the respective Codes of Conduct for employees (refer to **2. DEFINITIONS, Reasonable private use** previous in this General Order)
- any attempt to send SAPOL official information to an individual's private email account
- any attempt to synchronise a SAPOL email account with an individual's private email account.

Unauthorised material includes, but is not limited to, indecent, offensive, obscene or illegal material.

The definition of misuse does not apply where the material has been seized as evidence or obtained in the course of criminal investigations. Such material must be removed/disposed of, in compliance with the *State Records Act 1997* and the SAPOL Operational records disposal schedule (where the information forms part of an official record) as soon as practicable on completion of the investigation and any subsequent court action.

ALEIN (Australian Law Enforcement Intelligence Network) secure email system—an encrypted email system allowing secure communication between SAPOL and other policing jurisdictions.

3. ROLES AND RESPONSIBILITIES

All employees

An employee must do everything within their authority to prevent, and report, the loss, damage, or misuse of any element of or involvement in any prohibited act on SAPOL's email systems and must not damage, misuse or engage in any prohibited act on those systems.

Where material seized for evidence or obtained as outlined in **2. DEFINITIONS, Misuse** previous in this General Order is to be removed, the guidance of the senior forensic computing analyst should be followed.

Secure email system users

Employees exchanging classified material through the secure email system must adhere to all information security best practices. In addition to all General Orders relating to information technology and security, the following applies to the use of the secure email system:

- exchange all *Protected* (and higher classification) emails **only** through the secure email system
- do not discuss the content of secure email with other employees/persons who were not recipients
- do not leave the secure email system open on an unlocked and unattended computer
- always log out of the secure email system when finished working with secure email

- always be aware of other employees/people viewing the screen in a common area as other employees/people may not hold an appropriate security clearance for the data being accessed
- apply common sense to all situations.

When a security incident or information disclosure occurs it must be reported in accordance with General Order, **Protective security** (relative to security incidents and investigations). Additionally, the following notifications must be made immediately for:

- cyber security incidents—the IS&T Security Branch as directed within the IS&T *Security Incident Management Procedure*
- physical security incidents—the Agency Security Advisor by telephoning 820 74038 or emailing SAPOL.SEMSSecurityAdviceSection@police.sa.gov.au.

4. PROCEDURES

The following procedures apply to both general and secure email systems, unless stated otherwise.

Allocation of email accounts

General email accounts

Email accounts will be allocated by the Information Systems and Technology Service (IS&T) Service Desk upon receipt of an **Email Account Request (PD20)** which is to be submitted by the appropriate manager via the IS&T Self Service Portal.

Secure email accounts

Requests for secure email must be submitted using the **Secure Email - Access Request** via the IS&T Self Service Portal. The request must be approved by the employee's manager prior to the request being actioned.

Removal of email accounts

General email accounts

When an employee departs from SAPOL, their general email account will be deleted after 30 days of their SAPOL network account having being disabled.

Exceptions to this should be requested via email to IS&T Service Desk.

Secure email accounts

When an employee departs from SAPOL, an appropriate manager from their location is responsible for ensuring the IS&T Service Desk is advised so the secure email account can be disabled.

Group email

Group emails only apply to the general email system.

Due to their potential impact on the system, an employee must follow strict guidelines when sending group emails. A Service/District/LSA/branch may have a local policy governing the sending of group emails to another Service/District/LSA/branch, or within their own Service/District/LSA/branch. It is the employee's responsibility to check for local policy Service/District/LSA/branch requirements.

Emails to DL:SAPOL All Staff

A distribution list (DL) email message is:

- generally of an informational nature
- circulated to all employees by email
- generally authorised by an assistant commissioner/executive director or the Officer in Charge, Communications Group.

An assistant commissioner/executive director or the Officer in Charge, Communications Group is only authorised to approve a DL message that is routine and within their area of responsibility.

All DL messages that are significant and of a corporate nature must be approved by either the Commissioner of Police or the Deputy Commissioner. Significant messages are those of a special interest due to the circumstances in which they arise, for example a member killed or seriously injured on duty.

Details regarding sending an email to the whole of SAPOL are available through the intranet at <police connect home page/services/information systems and technology service/is&t service desk/applications/email/email – emailing sapol all staff>.

Whole of government emails (alert, notification and information messages)

Details regarding sending an email to the whole of government are available through the intranet at <police connect home page/services/information systems and technology service/is&t service desk/applications/email/email – email whole of government>.

An employee is expected to maintain their subscription to information messages issued from SAPOL. In accordance with the *SAPOL Leadership Charter* this will ensure all employees are aware of SAPOL-sponsored community events, initiatives and activities.

Outlook rules are not permitted to be setup to automatically delete whole of government emails.

User agreement

Access to SAPOL's information technology systems requires an employee's understanding and acknowledgement of correct system use as detailed in accordance with this General Order.

Employee inductions shall require the reading of this General Order prior to an employee accessing the general email system.

When secure email access is required, the employee shall submit a **Secure Email - Access Request** (via the IS&T Self Service Portal) which includes a User Agreement declaration and acknowledgement of a legitimate business requirement to transmit securely classified documents via secure email.

Monitoring

SAPOL may monitor the contents of any message or attachment stored on its computer system. Auditing the email system will provide authorised persons with all information relating to email messages including:

- addresses of senders and recipients, with transmission time and date
- content of email messages and attachments stored on email
- deleted and archived messages and attachments.

In addition to the ongoing reviews by IS&T and District/LSA/branch computer and systems audits, the Intelligence Analyst, Intelligence Section, Ethical and Professional Standards Branch will conduct random and targeted audits of the email system.

Management of emails as corporate records

SAPOL must maintain official records in accordance with the *State Records Act 1997*. Email can be considered an official record and as such all employees are responsible for ensuring that emails related to SAPOL business are printed and a copy attached to the relevant PCO, or alternatively retained electronically in the agency electronic document and records management system (TRIM) or business system.

Where there is an ongoing email exchange that constitutes an official record, it is the obligation of either the originator/sender (internal emails) or the recipient (external emails), to take responsibility for saving the entire email conversation by attaching to a PCO or retaining electronically, to ensure compliance with the *State Records Act 1997*.

SAPOL records can only be destroyed in accordance with a current and approved general disposal schedule (GDS) or records disposal schedule (RDS)—available through the intranet at <police connect home page/services/business service/ information services branch/records management unit>. Penalties apply for records destroyed without appropriate authorisation.

Emails must be individually assessed by their content and also against the GDS or RDS. Records Management Unit can be contacted for further advice.

Refer to *Management of Email as Official Records, Principles and Guidelines* (refer to **5. REFERENCES** further in this General Order).

General use of email system

As standard practice when sending email messages, the use of only authorised graphics, pictures and sound files should be used and must be kept to a minimum, as these files can overload the system. The following acts are specifically prohibited by employees when using either email system:

- establishing unauthorised connections
- destroying, altering, dismantling or re-configuring any part of the computer system
- attempting to test, bypass or defeat existing security controls
- circumventing or attempting to circumvent assigned limits, privileges or procedures
- disguising, or attempting to disguise, the type or nature of any unauthorised file or material stored or maintained on the computer system

- transmitting any material that is intended to arrange, promote or support industrial action as defined by the *Fair Work Act 1994* but does not include material in relation to approved committees which have been formed to provide consultation in industrial matters, such as workplace consultative committees
- using the computer system to devise or execute any criminal activity
- introducing, storing or transmitting any material that breaches any law, policy or principles relating to libel, discrimination, harassment or privacy
- concealing or misrepresenting their identity
- transmitting or publishing material in a manner that suggests it has SAPOL endorsement or a level of approval that it does not have
- propagating hoaxes or practical jokes.

Email security

Confidentiality of emails in the general email system cannot be guaranteed. SAPOL official records classified as *Protected*, as described in General Order, **Information—security classification**, must be sent through the secure email system provided the recipient at this or any other state or agency has the same or similar access.

Where an employee does not have access to this level of electronic messaging security then it must not be sent electronically. Such information, records or documents should then be sent by 'safe hand' or collected by the recipient to enable receipting of same.

Reasonable private use

The secure email system **must** only be used for business-related purposes. Employees sending emails that are not business-related must use the general email system.

All employees may use the general email system for reasonable private use, as defined at **2. DEFINITIONS, Reasonable private use** previously in this General Order, and subject to local instructions. Employees are not required to seek permission for each instance of private use.

An employee is responsible for complying with directions (in addition to those specified in this General Order) from their District/LSA/branch manager in regards to acceptable reasonable private use within the employee's current work environment.

All employees must comply with General Order, **Secondary employment** and General Order, **Secondary employment (Public Sector Act, Protective Security Act and weekly paid)** in relation to use of the email system.

In conjunction with the conditions specified at **2. DEFINITIONS, Reasonable private use** and in accordance with this General Order, an employee is to read the definition of secondary employment (in the relevant General Orders listed above) and note that:

- the use of any equipment belonging to or under the control of SAPOL is not permitted in the course of secondary employment; and
- they are not permitted to take part in any aspect of secondary employment whilst engaging in their SAPOL duties.

This **includes** sending and receiving emails.

It is the responsibility of the employee to inform parties associated with their secondary employment that they are not permitted to use their SAPOL email address in the conduct of their secondary employment.

Signature block

Each employee is responsible for ensuring that their email signature block conforms to the corporate branding signature block. Instructions for setting up the signature block are available through the intranet.

Disclaimer

A disclaimer will be placed on all outgoing messages sent from a SAPOL email account to protect SAPOL from possible legal action stemming from the content of messages. The disclaimer is the last paragraph in the email signature block, refer to **4. PROCEDURES, Signature block** previous in this General Order.

5. REFERENCES

Australian Government Information Security Manual (ISM)

Australian Government Protective Security Policy Framework (PSPF)

Code of Ethics for the South Australian Public Sector

Fair Work Act 1994

General disposal schedules are available through the intranet at <police connect home page/services/business service/information services branch/records management unit>

General Order, **Information—security classification**

General Order, **Records management**

General Order, **Secondary employment**

General Order, **Secondary employment (Public Sector Act, Protective Security Act and weekly paid)**

IS&T *Security Incident Management Procedure*

Management of Email as Official Records, Principles and Guidelines

Police Act 1998

Police Regulations 2014

Public Sector Act 2009

SA Government Cyber Security Framework (SA CSF)

SAPOL Operational records disposal schedule

South Australia Police Code of Conduct

South Australia Police Leadership Charter

State Records Act 1997

6. FURTHER ENQUIRIES

IS&T Service Desk telephone 732 23333.

7. DOCUMENT HISTORY SINCE 25/03/09

Gazette reference (SAPG)	Date	Action (amendment/deletion/new/review/temporary variation)
108/09	25/03/09	New General Order.
163/10	16/06/10	Amendment 2010.
214/11	27/07/11	Review 2011.
247/12	03/10/12	Amendment—Communications Branch has been renamed to Communications Group.
152/15	05/08/15	Review 2015.
161/16	03/08/16	Review 2016.
150/18	04/07/18	Amendment—district policing model implementation.
57/20	25/03/20	Review 2020—including references to the secure email system.
7/23	11/01/23	Review 2022—the process for requesting general and secure email accounts through the IS&T Service Portal has been added, including the removal of the requirement to submit a **PD20 SAPOL Email and Internet User Agreement and Secure Email User Agreement**. The process for the removal of general email accounts and user agreement requirements have been updated. The example signature block has been removed.

APPROVED BY COMMISSIONER/DEPUTY

…… ……
Print Full Name *ID Number*

…… 30/12/22
Signature *Date*

Documentation certification and verification

General Order draft—prepared by: Christine Barnden, Technical Writer, Security Branch, Information and Systems Technology Service; Karen Washington, Manager, Customer Service Branch, Information and Systems and Technology Service

General Order—verified by: Hamish Cameron, Executive Director, Information Systems and Technology Service