Victoria Police Manual – Procedures and Guidelines

Use of email

Policy Link

These Procedures and Guidelines support and must be read in conjunction with the following:

- VPMP Information access
- VPMP Appropriate use of information

The following references provide additional information or requirements of relevance:

- VPMP Information categorisation, collection and recording
- VPMP Information use, handling and storage
- VPMP Information sharing
- VPMP Information review, retention and disposal

Application

Procedures and Guidelines are provided to support the interpretation and application of rules and responsibilities. They include recommended good practices and assessment tools to help employees make lawful, ethical and professional decisions. Employees should use the **Professional and ethical standards** to inform the decisions they make to support interpretation of Procedures and Guidelines.

Procedures and Guidelines are not mandatory requirements on their own. However, where rules and responsibilities state that employees must have regard to Procedures and Guidelines, the Procedures and Guidelines must be used to help make decisions in support of the rules.

Procedures and Guidelines

1. Overview

- Email is an essential tool for the conduct of Victoria Police activities and communication.
- There are risks associated with email which have to be actively managed, including but not limited to:
  - increased difficulty in controlling record keeping and legal liability issues

- email not being a secure form of communication, and an inability to guarantee privacy and confidentiality
- problems related to information overload, inevitable when large quantities of information, some of which is of marginal value, is delivered to individuals.

2. Authorised Users' responsibilities

- As detailed in **VPMP Appropriate use of information**, all Authorised Users must be aware of their responsibilities when using Victoria Police information or information systems.

- When using the Victoria Police email, Authorised Users are to comply with this guideline, VPM policies for handling information and any local instructions.

- Email is used within Victoria Police as a tool for communication, advice and tasking. Therefore all Authorised Users are required to read their email regularly to ensure that important information is received in a timely manner.

3. Use of email

3.1 Appropriate communication tool

- Before using email, consider whether it is the most appropriate method of communication. If immediate action is required, direct contact with the recipient such as by phone, may be more suitable.

- Emails sent as an 'FYI' should be kept to a minimum. Authorised Users should only send or forward email messages to recipients who have responsibility for the issue or who are expected to act on the message.

- The Victoria Police email system is only rated to send internal mail **below** PROTECTED – i.e. UNCLASSIFIED with or without Dissemination Limiting Markers such as 'For Official Use Only' or 'Sensitive: Personal'.

3.2 Information protective markings

- Information protective markings are security classifications or other Dissemination Limiting Markers such as 'For Official Use Only'.

- Authorised Users must be conscious of any protective markings or handling requirements for the information and determine if email is a suitable form of transmission. Refer to **VPMP Information use, handling and storage** for more information on appropriate transmission methods.

- Protective markings should be included in both the subject field and message body of the email.

- A Victoria Police approved legal disclaimer is automatically placed on all emails going outside the Victoria Police network. Users should not include alternative legal disclaimers in their signature blocks.

- The electronic transfer of protectively marked information is dependant upon the recipients need to know, and the intent of the protective marking.

- In accordance with **VPMP Information use, handling and storage**, any information with a security classification must have additional security measures, including encryption, to protect the information contained in the email. Refer to the table below for more information.

Dissemination Limiting Markers or Security Classification	**Electronic transfer requirements**
CONFIDENTIAL, SECRET and TOP SECRET (or legacy RESTRICTED or HIGHLY PROTECTED)	• Internal/External: Not to be sent via the Victoria Police email system
PROTECTED	• Internal: Encryption required if being sent via the Victoria Police email system to other **.gov.au** domain email accounts. • ALEIN can be used for this material • External: Not to be sent to external email accounts
UNCLASSIFIED 'For Official Use Only' or other Disseminating Limiting Marker	• Internal: Can be sent via the Victoria Police email system to other **.gov.au** domain email accounts. • External: Encryption should be considered depending on the information content and the recipient.
PUBLIC DOMAIN	• Internal / External: Can be sent via the Victoria Police email system.

- Refer to **VPMP Information use, handling and storage** for details on requirements for transmitting security classified material by email.

- ALEIN can be accessed from the Applications intranet page. For creation of accounts please contact the Intelligence Collection and Liaison Unit.

3.3 Email size limits

- The size limits on external emails are:
  - messages between 0 to 5 MB (megabytes) will send automatically
  - messages between 5 and 10MB are parked. This means they are put in a 'holding bay' and sent at an off-peak time.
  - messages 10 MB and above will not be sent. The sender of the oversize message will be notified with an error message.

3.4 Email attachments

- Large files (5MB or over), particularly images or audio/visual material, should not be sent via email unless it is an urgent operational requirement.

- Alternatives for the distribution of email attachments, appropriate to the security classification of the material, should be considered. This could include:
  - saving the file on a shared network drive and emailing a link to the file (For details on how to send a link please refer to the **Protective Security guide - G180 - Managing Outlook email and calendar**).
  - hand delivery of the file on a disk
  - loading the file onto the Intranet
  - loading the file into an appropriate corporate application.

3.5 Official records management

- Email messages sent or received on the Victoria Police IT system are public records under the *Public Records Act 1973* and as such they must be managed in line with the Public Records Office of Victoria (PROV) standards.

- To comply with **VPMP Information categorisation, collection and recording,** email records that contain a business decision and/or business transaction must be printed and attached to a Force File or other relevant file.

- The Victoria Police email system or email archive are not PROV approved record keeping systems.

- Victoria Police does not currently use a PROV approved electronic record keeping system.

3.6 Management of email

- Authorised users should take steps to manage and use their email accounts effectively. This includes:

- providing their supervisors or managers with any relevant information they have in their email account when they will be absent from duty or leaving the organisation
- performing regular maintenance of their account, including deleting email in line with the following table:

Email content	Delete	Timeframe
Work related transitory message of minor importance	Once their administrative value ceases	Preferably prior to inclusion in email archive
Work related message of continuing value	Only once a copy has been captured in the relevant official record-keeping system	N/A
Personal message	As soon as possible	Prior to inclusion in email archive

- arranging alternatives for the management of their account when they will be absent from duty, such as using 'Out of Office' messages or providing other users access to their Inbox through the 'sharing' function within Outlook. Refer to the **Protective Security guide - G180 - Managing Outlook email and calendar** for advice on how to do this securely.

- Auto-forward functions should be used carefully, so that sensitive information is not forwarded to persons who should not view it.

- Auto forward functions are not to be used to forward Victoria Police email messages to an external email account.

- In accordance with **VPMP Information access**, logon details must not be provided to any other individual, including providing access to email accounts.

3.7 Email archive

- Victoria Police currently utilises an email archive system. This system is not an official record system, but provides a searchable archive facility for the convenience of Authorised Users.

- Once an email has been included in the email archive, it remains in the archive until deleted by IT. Authorised Users may delete the email from their view of the archive, however it will remain in the archive.

- As access to archived emails is user specific, emails should be transferred to other electronic storage or official record keeping system prior to inclusion in the archive.

- Unofficial or transitory messages of minor importance should be deleted from an Authorised User's account (inbox and sent items) prior to inclusion in the email archive. Email messages will automatically be included in the archive after 30 days or after 7 days if the message is larger than 1MB.

3.8 Personal use of email system

- The Victoria Police email system may be used for personal email in accordance with **VPMP Appropriate use of information**.

- Authorised users are to ensure that personal emails are clearly identified as being from the individual and are not sent as a representative of Victoria Police. For example include a 'Personal' label in the subject line and do not use position or an official signature block.

3.9 General operational and corporate messages

- General operational or corporate messages should not be widely distributed by email.

- Authorised Users should consider alternative methods of distributing the information, including publishing the information on the intranet.

- **VPMG Internal information distribution** provides more guidance on the appropriate methods of communication and associated approvals for wide distribution of information by email.

3.10 Email signature blocks

Email signature blocks must be consistent with the standard set out in the **Victoria Police Style Guide**. They must be concise, include name, position, work location and contact details. They must not include personal information, quote, taglines, images or animations.

4. Position based email accounts

- Work Unit Managers should consider establishing and maintaining a Position Based Email Account (PBEA) to facilitate the dissemination and exchange of information. Apply for the creation of a PBEA via the InsighT Portal Self Service Application.

- The primary owner of the PBEA is responsible for:
  - management of the account and assigning permissions to other authorised users
  - ensuring that management responsibilities are transferred to a delegate with similar access levels when going on leave or temporary absence

  - ensuring that ownership of the account is transferred when leaving the position, by completing a Request for Transfer of Ownership of a PBEA via the InsighT Portal Self Service Application.

- The Director, IT Service Request Centre is responsible for ensuring compliance to the naming convention and security of PBEAs according to established Data Standards.

5. Monitoring and Security

5.1 Monitoring of messages

- As detailed in **VPMP Appropriate use of information**, any personal information created, stored and/or transmitted on Victoria Police information systems will be treated as Victoria Police information.

- Any email sent to or from Victoria Police may be monitored either through automatic filters or via manual analysis. These messages are not private and are the property of Victoria Police and/or the Victorian government.

- If an Authorised User does not want personal information to be accessible to supervisors, investigators, auditors and system administrators, then the Victoria Police email system is not an appropriate way to transmit the information.

5.2 Email filtering and spam

- Victoria Police uses an email protection service to filter and quarantine all incoming and outgoing internet email to protect the organisation from potentially harmful threats. Advice on how to release emails that have been quarantined can be obtained from the Spam Quarantine Report intranet page.

- Authorised Users should not solicit large volumes of incoming mail with no, or marginal, relevance to their role with Victoria Police. Victoria Police reserves the right to request that users unsubscribe from external mailing lists.

- If you receive an email that you consider as spam please report it to allow the filtering system to block future emails of this type. Advice on how to report spam can be obtained from the Email Spam intranet page.

5.3 Suspicious emails

- Should an employee receive an email that is unexpected, suspicious or that suggests an unusual course of action, recipients should seek to verify the authenticity of the message via some other form of communication. This may take place via personal contact, paper mail, fax, telephone, or another authentication means.

- Authorised Users should not click on links, reply to or open attachments on suspicious emails.

5.4 *Inappropriate or offensive content*

- In line with **VPMP Appropriate use of information**, Authorised Users must not create, copy, forward or store email messages that contain inappropriate or offensive material, or links to such material or websites (unless authorised for legitimate work duties). This includes but is not limited to:

  - material containing any discriminatory or vilifying language, images or sounds relating to individual or groups personal characteristics, whether actual or presumed, including sex, race, disability, physical features, sexual orientation, gender identity, religious or political beliefs, national origin, marital or parental status, pregnancy or breastfeeding, or age
  - the circulation of any material which would constitute a breach of the *Equal Opportunity Act 2010 (Vic)* and or the *Racial and Religious Tolerance Act 2001 (Vic)*
  - the circulation or disclosure of any material which would be incompatible with a person's human rights under the *Charter of Human Rights and Responsibilities 2006 (Vic)*
  - obscene, pornographic, erotic, sexually explicit, violent, defamatory, offensive, insulting, threatening or harassing language, images or sounds
  - any other material which a reasonable person would find offensive.

  Use of the email system in contravention of this direction is regarded as particularly serious and may lead to disciplinary consequences including termination of appointment. The nature of the material and the extent of its circulation, rather than the category into which it falls, will determine the seriousness of the contravention.

- If an email is received from a known sender, such as a friend or colleague, that contains inappropriate or offensive material, or links to such material or websites, it is recommended that the recipient asks the sender not to send this type of material in future via some other form of communication. This may take place via personal contact, paper mail, fax or telephone.

5.5 *Inappropriate use or security breaches*

- In line with **VPMP Protective security incident reporting and management**, Authorised Users are required to notify their Work Unit Manager of any perceived misuse of the email or system security breaches, including viruses.

- If an Authorised User is believed to have used their email inappropriately, access may be withdrawn pending investigation.

- If email access is withdrawn, it may be restored by completing a Form 1250 at the discretion of the Authorised User’s Work Unit Manager or Professional Standards Command (PSC) (depending on the severity of the breach).

5.6 Access to another Authorised User’s email account

- If an Authorised User needs ongoing or temporary access to another Authorised User’s email account, this should be provided by using the permission settings within the email account. Refer to the **Protective Security guide - G180 - Managing Outlook email and calendar** for advice on how to do this securely.

- If this is unable to occur (i.e the member is on extended leave), Supervisors or another Authorised User may request access to the email account, provided they have a legitimate business reason for doing so and are in a role appropriate to the business reason.

- Two (2) levels of approval for the access are to be documented prior to submitting a request for access via Form 1234:
  - approval from the requestor’s Supervisor, and
  - approval from the Supervisor’s Supervisor.
- The request and approvals are to include:
  - the V or VP numbers, positions and the Authorised User’s full names
  - reason for the access
  - activity to be carried out
  - length of time access is required so that access is removed when the task is completed
- The documented approvals are to be included as an attachment to Form 1234. If approvals are sought via email, the full email trail is to be included.

6. Exemption

If an Authorised User or work area requires an exemption from the requirements of any part of the referenced Policy Rules or these Guidelines for a specific business reason, they require written approval from their Work Unit Manager, Department Head and the IT Security Advisor (IT-SECURITY ADVISOR-MGR).

Further Advice and Information

For further advice and assistance on using email in line with these Procedures and Guidelines, speak to a supervisor or your Ethical & Professional Standards Officer.

Update history

Date of first issue	15/10/13	
Date updated	**Summary of change**	**Force File number**
27/11/13	Reference to redundant instrument in Section 3.2 updated with replacement instrument.	FF-075739
30/03/15	Inclusion of guidelines about email signature blocks standards.	FF-088701
30/08/16	References to VP forms for requesting Position Based Email accounts were replaced with self- service request through the InsighT Portal application.	FF- 041069/05 and FF- 041056/05
25/03/19	Administrative amendments to reflect name change from IMSSD to Protective Security.	FF-139207