Use of internet

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. 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.

- Employees are reminded that the provisions of the *Victoria Police Act 2013* apply to all police employees, both current and former. It is an offence to access, make use of or disclose police information if you are not authorised to do so. This provision applies at all times and is inclusive of employees'

use of official or private email accounts, social networking and other internet services/systems.

- Police information must not be stored or transmitted using internet based systems or accounts unless specifically authorised by the Information Management Committee.
- When using the Victoria Police IT systems to access the internet, Authorised Users must comply with VPM policy/guidelines and any local instructions.

2. Internet usage

2.1 Internet restrictions

- When using the Victoria Police IT system Authorised Users must:
  - only use authorised tools to access the internet
  - only use authorised official gateways/links to access the internet
  - not access web based e-mail services
  - not intentionally download, save or install software or files that are unauthorised, unlicensed, subject to copyright fees, may introduce malicious software and/or are from blocked sites.
- At all times Authorised Users must:
  - not transfer official information via online services (cloud storage services or software as a service) unless the service has been approved by the Information Management Committee
  - only use social media in line with **VPMG Social media and online engagement** and **VPMP Appropriate use of information**.
- Internet use from the Victoria Police IT system is partly managed through internet browsing rules, which categorise websites as:
  - unrestricted – sites are available to users with no system limitations
  - restricted – use of sites is capped at 2 hours per day
  - blocked – sites cannot be accessed.
- Further details of the categorisations can be found on the intranet on the Website Categories and Restrictions page.

2.2 Development of websites

- In line with **VPMP Corporate communications**, employees must not develop personal internet sites or home pages that:
  - could be identified as representing or associated with Victoria Police
  - use official Victoria Police information.
- All official websites, accounts or pages that represent Victoria Police must be approved by Media & Corporate Communications Department and the Infrastructure Department in accordance with **VPMP Corporate communications**.

2.3 Reputation management

- Employees need to be mindful of how they communicate over the internet, including online social networking, dating or other internet sites, in terms of their safety, reputation and reputation of the organisation. Employees should demonstrate due care when considering the information they place on such sites to reduce the risk of such information being accessed by an unintended audience and/or for unintended purposes.

- When using internet services, it is recommended that employees:
  - use appropriate security/privacy settings
  - do not reveal or discuss details of their employment, place of work or duties (including logos, images or online forum posts/discussions)
  - do not reveal their address, or other details that may enable unsolicited contact
  - only post material that does not compromise their reputation or integrity or that of the organisation.

- See **VPMG Social media and online engagement** for further guidance on using social media in either a personal capacity or as an authorised representative of Victoria Police.

3. Monitoring

3.1 All information

- Any internet access from Victoria Police may be monitored. Activities on the Victoria Police IT network, including internet browsing, are not private and may be subject to scrutiny by supervisors, investigators, auditors and system administrators for any reasonable purpose.

- 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.

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

3.2 Inappropriate or offensive content

- In line with **VPMP Appropriate use of information**, Authorised Users must not intentionally access, download, transmit or save any data from the internet onto the Victoria Police IT network or storage media that contains 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 group 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 IT system in contravention of this direction is regarded as particularly serious and may lead to disciplinary consequences including termination of appointment. The seriousness of the contravention will depend on the nature of the material and the extent of access, storage or circulation, rather than on the category into which it falls.

3.3 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 internet or system security breaches, including viruses.

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

- Internet access may be restored by completing a Form 1250, once Professional Standards Command advises the relevant Department Head and the System Sponsor that access may be restored.

4. Exemptions

4.1 Authorised access

- If an Authorised User or work unit 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 and Department Head. This approval is to be provided to the IT Security Advisor (IT-SECURITY ADVISOR-MGR).

- If an Authorised User or work unit requires access to blocked or restricted websites, they are to complete and submit a Request for Exemption to Internet Browsing Rules [Form 1036A].

- The maximum period for an exemption is 12 months. Authorised Users who have been granted an exemption will receive an email alert before their exemption expires.

- Refer to **VPMP Information access** regarding Authorised User and Work Unit Managers' responsibilities for revising, revoking or removing access when it is no longer required.

4.2 Stand-alone access

- Use of a stand alone system to access the internet by an employee or work unit requires approval from the Work Unit Manager, Department Head and the Information Technology Security Advisor. Approval to use a stand-alone computer is to be subject to the following conditions:
  - it is not be connected to the Victoria Police IT network at any time
  - it is to have current Victoria Police approved anti-virus protection installed and active
  - unauthorised individuals are not to have access to the equipment (including for repair or maintenance)
  - equipment is to be appropriately destroyed at the end of its useful life in accordance with **VPMG Information and information equipment disposal**
  - access to and use of the system is to be recorded for audit purposes. This is to include time and date, details of the user and reason for access.

- Stand alone computers are not to be used to hold any Victoria Police information for personal purposes or for police work that should be done on the Victoria Police IT system.

- The work unit is responsible for arranging access through an external internet service provider and for costs involved in doing so.

Further Advice and Information

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

Update history

Date of first issue	14/10/13	
Date updated	**Summary of change**	**Force File number**
05/08/14	Minor amendment updating reference to *Victoria Police Act 2013*, as this replaces the *Police Regulation Act 1958*	N/A