



---

# Information Technology & Confidentiality Policy

---

Australian Peacekeeper and Peacemaker Veterans' Association  
ACN 651 805 702

Adopted on 3 September 2021

# Information Technology & Confidentiality Policy

Australian Peacekeeper and Peacemaker Veterans' Association Ltd ACN 651 805 702 (**APPVA**)

---

## **A. POLICY PRINCIPLES**

### **1. Application And Enforceability**

---

1.1 This Policy applies to APPVA and to Users of APPVA Information Technology ('IT') Facilities.

1.2 This Policy:

(a) Is informational in terms of:

(i) how APPVA may operate and monitor IT Facilities; and

(ii) what APPVA may do to address matters relating to Confidential Information and Intellectual Property.

APPVA's core obligations are contained in the Relevant Legislation, not this Policy;

(b) Is directional where it refers to what Users must do or not do; and

(c) Is not contractually enforceable against APPVA.

### **2. Our Policy**

---

2.1 APPVA provides IT Facilities and Confidential Information to Users for the purpose of APPVA business.

2.2 This Policy covers:

(a) Appropriate use by Users of our IT Facilities;

(b) Security of IT Facilities and Confidential Information; and

(c) Monitoring by APPVA of IT Facilities.

## **B. USE OF IT FACILITIES**

---

### **3. Appropriate Use**

---

3.1 Users must:

(a) Only use the IT Facilities for the purpose of APPVA's business interests (with the exception of reasonable personal use referred to at clause 4.1), consistent with:

(i) The services APPVA provides to its clients or customers;

- (ii) The specific objectives of any given task you are instructed to perform; and
- (iii) The efficient and productive administration and running of APPVA's business.

## **4. Personal use**

---

- 4.1 Users are permitted to use the IT Facilities for limited and reasonable personal use, subject to the following:
- (a) Personal use must not detract from the due performance of your duties or the duties of any other volunteer or employee;
  - (b) you must not use the IT Facilities during your ordinary working hours (excluding lunch break) or at times in which you should be engaged in the performance of your duties;
  - (c) You must not use the IT facilities to:
    - (i) Play games;
    - (ii) Access or use gambling sites;
    - (iii) Access or use social networking sites, such as facebook, twitter and instagram;
    - (iv) Access or use video and music sharing sites such as youtube;
    - (v) Access or use webmail sites such as hotmail, yahoo and gmail;
    - (vi) Solicit, store or send unnecessary or frivolous emails (e.g. Spam, chain letters or junk mail) or click on 'click-bait' or popup advertising; and
  - (d) APPVA is not responsible for the security of any personal information stored or otherwise connected to the IT facilities. Any personal information and material you have stored on APPVA IT facilities may be removed without notice. APPVA does not guarantee the availability of it facilities. They may be unavailable without notice from time to time.

## **5. Prohibited & Required Conduct**

---

- 5.1 You must not:
- (a) Use IT Facilities to engage in conduct that is prohibited under any of APPVA's other policies and procedures, including the Bullying, Harassment & Discrimination Policy and the Social Media Policy;
  - (b) Use, access or modify APPVA IT Facilities, Confidential Information, records or passwords without prior express authorisation from APPVA;
  - (c) Engage in conduct that reasonably could or does:
    - (i) Damage the IT Facilities or records of APPVA (including physically or by opening or downloading electronic messages or files that could reasonably be suspected of having a virus attached); and
    - (ii) Impair or interrupt the normal services of the IT Facilities (e.g. Creation of heavy network traffic, printing large volumes of unnecessary material, unnecessary

saving of large files or information, or clicking on pop-up advertising links that may contain a virus);

- (d) Use IT Facilities to access, store, transmit or engage in:
  - (i) Any form of unlawful or prohibited conduct as prescribed under Australian laws, included but not limited to the Relevant Legislation;
  - (ii) Any offensive or objectionable conduct or material (including material of a sexual nature, pornography, violent material, offensive jokes or material that instructs, incites or contains criminal behaviour);
- (e) Install software or run programs on the IT Facilities without the prior authorisation of APPVA (the type of programs included in this prohibition include, but are not limited to software known as viruses, trojan horses, worms, password breakers, spyware and packet observers);
- (f) Connect any devices to the IT Facilities that are not authorised by APPVA, including:
  - (i) External USB sticks or flash drives, including that may contain unlawful or objectionable material, or that may contain a virus; or
  - (ii) Any electronic device that has the capacity to monitor, intercept, copy or transmit data or any other form of information that can be transmitted electronically; and
- (g) Use the IT Facilities to infringe someone else's Intellectual Property, including Copyright Material, without permission from the owner. Copyright Material can be infringed including by:
  - (i) Using a 'substantial part' of the work, including by paraphrasing or mirroring the structure of a document (including by failing to attribute or falsely attributing the creator of the work), regardless of whether you or APPVA is profiting from the use of the Copyright Material;
  - (ii) Importing or selling infringed Copyright Material; or
  - (iii) Copying or unauthorised distribution or alteration of computer software, except in accordance with a license or service agreement.

## 5.2 You must:

- (a) Implement and use any virus protection measures as directed by APPVA from time to time; and
- (b) Adhere to the software vendors' license agreements that APPVA has with software providers except as permitted by law or by contract with the owner of the copyright.

## 5.3 You must ensure that electronic mail and short message service (SMS):

- (a) Messages are courteous and polite and do not contain obscene, offensive or slanderous material. If you receive unsolicited emails which breach this Policy or any other APPVA policy, you must not forward such emails, must delete them, and must take reasonable steps to prevent a recurrence;
- (b) Messages contain the APPVA standard email signature and disclaimer;
- (c) Messages do not conflict with APPVA interests or contain information that is harmful to APPVA; and
- (d) 'out-of-office' settings are used for any periods of absence.

## **C. SECURITY OF IT FACILITIES AND OF CONFIDENTIAL INFORMATION**

---

### **6. Security of Confidential information**

---

- 6.1 Safeguarding APPVA's Confidential Information and Intellectual Property is a joint responsibility of every User. Accordingly, you must:
- (a) Store all Confidential Information in the appropriate location as directed by APPVA;
  - (b) Maintain the security of all IT Facilities and Confidential Information from unauthorised access, use, copying or disclosure;
  - (c) Use all file security mechanisms built into APPVA IT Facilities, as required or directed by APPVA including by saving backups, and running virus and system checks; and
  - (d) Not access, use or copy the personal information of other Users unless authorised by them or APPVA;
  - (e) Not appropriate, copy, destroy, damage, memorise or in any manner reproduce any of APPVA Confidential Information without APPVA's prior written authorisation;
  - (f) Not access or disclose APPVA Confidential Information or permit any person or entity to access or use any of APPVA Confidential Information, without APPVA prior written authorisation;
  - (g) Not use any of APPVA's Confidential Information for any purpose other than for the benefit of APPVA business or otherwise seek to exploit APPVA's Confidential Information;
  - (h) Not remove any of APPVA IT Facilities (including mobile telephones or laptops) or Confidential Information from APPVA's premises without APPVA's prior written authorisation;
  - (i) Not access the IT Facilities or Confidential Information from any personal device (including mobile telephones and laptops) without APPVA's express authorisation; and
  - (j) Maintain the security of any personal devices with access to the IT Facilities or Confidential Information, including by ensuring the device is password protected and has virus protection and security systems acceptable to APPVA.
- 6.2 On APPVA's request you must immediately return all of APPVA Confidential Information in your possession to APPVA.
- 6.3 If required by APPVA, you must also sign a confidentiality undertaking and non-disclosure agreement in respect of APPVA Confidential Information.

### **7. password security**

---

- 7.1 You must maintain password security including by:
- (a) Using a strong password that conforms to the APPVA computer password policy;
  - (b) Saving passwords in the APPVA approved password manager;
  - (c) not writing down or saving your password anywhere including on the IT Facilities or sharing it with anyone outside APPVA;

- (d) Not disclosing your password to anyone inside APPVA, or obtaining another User's password to access IT Facilities;
- (e) Changing your passwords every three months; and
- (f) Not giving your passwords to your anyone else.

## **8. Reporting Requirements**

---

- 8.1 You must notify the Company Secretary immediately if:
- (a) You suspect or become aware that this policy has been breached;
  - (b) Sensitive or confidential information, passwords or other it facility access or control has been or is suspected of being lost or disclosed to unauthorised parties;
  - (c) There is any unusual systems behaviour, such as missing files, frequent system crashes or misrouted messages; or
  - (d) If you receive a threat of an electronic nature, e.g. a computer virus warning.

## **D. MONITORING IT FACILITIES**

---

### **9. Monitoring and access**

---

- 9.1 Subject to clause 10.2, APPVA IT Facility system logs and records all information of its Users' activities on a continuous and ongoing basis including in relation to:
- (a) The content of, and user access to, IT Facility storage volumes;
  - (b) Websites that are visited;
  - (c) Any information or material that has been downloaded;
  - (d) Suspected malicious code or viruses;
  - (e) The content of all emails received, sent and stored on the computer network (including emails deleted from a user's inbox); and
  - (f) IT Facility hardware.
- 9.2 The monitoring and examination of IT information will be carried out by staff authorised by APPVA. Only those authorised persons will have access to this information.
- 9.3 APPVA may monitor and use the information set out in clause 9.2 at any time and without further notice to any User of its IT Facilities. APPVA may use or disclose the information for the following purposes:
- (a) To ensure your compliance with this Policy or any other policy of APPVA;
  - (b) For any reason relating to APPVA business activities, including taking adverse action against you;
  - (c) As response to a request by a law enforcement agency in connection with an alleged offence;

- (d) For disclosure in connection with legal proceedings; or
- (e) Because it is reasonably believed to be necessary to avert an imminent threat of serious violence to any person or substantial damage to property.

9.4 APPVA reserves the right to limit or restrict, permanently or temporarily:

- (a) Your use or access of APPVA IT Facilities;
- (b) any Electronic Communication; and
- (c) Your ability to copy, remove or otherwise alter any information or system that may undermine the authorised use of APPVA IT Facilities;

With or without notice to you.

9.5 APPVA reserves the right to take emergency action to safeguard the integrity and security of APPVA IT Facilities. This includes but is not limited to the termination of a program, job or on-line session, or the temporary alteration of user account names and passwords. The taking of emergency action does not waive APPVA's rights to take additional action under this Policy.

9.6 A stopped delivery notice will be given to a User if an Electronic Communication is stopped, except:

- (a) to stop or prevent Electronic Communication that APPVA believes:
  - (i) Is spam;
  - (ii) Might damage the IT Facilities; or
  - (iii) Might reasonably contain threatening, harassing or offensive communications or attachments;
- (b) Where the Electronic Communication is stopped by operation of a software program designed to stop the types of communications listed above; or
- (c) Where APPVA could not reasonably know that the worker sent the Electronic Communication.

9.7 Electronic Communications and internet access containing information relating to industrial matters will not be stopped by reason of such content alone.

## **10. Listening Devices**

---

10.1 Users must not:

- (a) Listen to or record a private conversation to which they are not a party; or
- (b) Record a private conversation to which they are a party.

10.2 APPVA will not record user's private conversations.

## **E. DISCIPLINARY SANCTIONS**

---

### **11. Misconduct**

---

11.1 A breach of this Policy may amount to volunteer/employee misconduct resulting in a range of disciplinary sanctions, including but not limited to:

- (a) A requirement to attend counselling or training;
- (b) A formal warning noted on the worker's personnel file;
- (c) The requirement to make verbal or written apology; and/or
- (d) Termination of employment.

11.2 APPVA underperformance and misconduct policy sets out APPVA policy in relation to misconduct.

## **F. DICTIONARY**

---

### **12. Definitions**

---

12.1 In this policy, words defined in the Relevant Legislation have the meaning given by that legislation, a number of which (as underlined> are set out in broad terms below. Words within this Policy have the following meanings:

- (a) 'Australian Peacekeeper and Peacemaker Veterans' Association' means Australian Peacekeeper and Peacemaker Veterans' Association Ltd ACN 651 805 702;
- (b) 'Confidential Information' includes any information which is confidential to APPVA or which APPVA states is confidential including but not limited to:
  - (i) Information that is marked 'Confidential' or which is described or treated by APPVA as confidential;
  - (ii) The Confidential Information of the entities associated with APPVA;
  - (iii) The Confidential Information of any of APPVA related bodies corporate;
  - (iv) The personal or Confidential Information of all members, stakeholders, clients of APPVA or potential clients of APPVA including their names, addresses, phone numbers or contact details;
  - (v) APPVA trade secrets, Copyright Material, Intellectual Property, know-how, techniques, designs, plans and models;
  - (vi) APPVA business systems including any procedure or process that APPVA uses as a delivery mechanism for providing its services to clients (including potential clients) including information about the method of presentation, manufacture or supply of goods or services by APPVA, quality assurance checklists, procedures, techniques and work methods; and



- (vii) Without limiting the generality of the above, the following specific confidential information, provided it has not been made generally known by APPVA to the public:
  - A. Internal email, memoranda and correspondence;
  - B. Information of a business sensitive nature;
  - C. APPVA computer programs, including their use, processes and functions;
  - D. Information related to the terms upon which APPVA contracts or provides services to clients, including but not limited to pricing information;
  - E. Information related to the terms upon which APPVA contracts or receives goods or services, including but not limited to pricing information;
  - F. APPVA business plans, marketing plans and forecasts;
  - G. APPVA financial circumstances;
  - H. Personal details of any APPVA volunteer employee or contractor;
  - I. The terms upon which APPVA engages volunteers, employees or contractors, including fees, commissions and remuneration packages; and
  - J. Client lists;
- (c) 'copyright material' includes literary, dramatic, musical or artistic work or a cinematograph film that the creator has exclusive rights to license to others. Copyright material does not need to be registered or published in order for copyright to attach to the work;
- (d) 'Employee' means a volunteer, employee, contractor or sub- contractor using VST IT Facilities;
- (e) 'electronic communication' means communication by electronic means including email and instant messaging;
- (f) 'intellectual property' includes patents, registered and unregistered trademarks, designs know-how and copyright material as defined by Australian law;
- (g) 'it facilities' means the systems, computers and telecommunications equipment used, owned or operated by APPVA, regardless of their location, including:
  - (i) The telecommunications network, including any local area network or wide area network (e.g. The internet and the intranet);
  - (ii) Devices, hardware or equipment including computers, laptops, tablets, tablet computers, telephone systems;
  - (iii) Computer software including computer programs, libraries and their associated documentation, files and stored information; and
- (h) 'policy' means this information technology & confidentiality policy;

- (i) The 'relevant legislation' means the legislation defined in the table at the front of this policy;
- (j) 'user' or 'you' means a person who carries out work in any capacity for APPVA, including work as:
  - (i) A volunteer;
  - (ii) An employee;
  - (iii) A contractor or subcontractor;
  - (iv) An employee of a contractor or subcontractor;
  - (v) An employee of a labour hire company who has been assigned to work for APPVA;
  - (vi) An outworker;
  - (vii) An apprentice or trainee;
  - (viii) A student gaining work experience;
  - (ix) A commission agent, meaning a person who does work for another person as the agent of that other person and who is remunerated, whether in whole or in part, by commission;
  - (x) A partner in a partnership; or
  - (xi) Any guest or person who is authorised or permitted to use APPVA it facilities.

<b>Title</b>	Information Technology & Confidentiality Policy		
		<b>Issue date</b>	
<b>Jurisdiction</b>	Commonwealth	<b>Version</b>	1
<b>Relevant Legislation</b>	<p>Commonwealth:</p> <ul style="list-style-type: none"> <li>- <i>Copyright Act 1968</i></li> <li>- <i>Copyright Amendment (Digital Agenda) Act 2000</i></li> <li>- <i>Crimes Act 1914</i></li> <li>- Commonwealth and Territory legislation listed in the Bullying, Harassment &amp; Discrimination Policy</li> <li>- <i>Privacy Act 1988</i></li> </ul> <p>Australian Capital Territory:</p> <ul style="list-style-type: none"> <li>- <i>Crimes Act 1900</i></li> <li>- <i>Workplace Privacy Act 2011</i></li> <li>- <i>Listening Devices Act 1992</i></li> </ul> <p>New South Wales:</p> <ul style="list-style-type: none"> <li>- <i>Crimes Act 1900</i></li> <li>- <i>Privacy and Personal Information Act 1998</i></li> <li>- <i>Workplace Surveillance Act 2005</i></li> <li>- <i>Surveillance Devices Act 2007</i></li> </ul> <p>Queensland:</p> <ul style="list-style-type: none"> <li>- <i>Criminal Code Act 1899</i></li> <li>- <i>Information Privacy Act 2009</i></li> <li>- <i>The Invasion of Privacy Act 1971</i></li> </ul>		