

## 5.01 Information Technology Policy and Procedures

**Authority:** Chief Executive Officer

**Issue Date:** October, 2018

**Review Date:** October 2021

### VERSION CONTROL

Date	Version	Author	Comments
October 2018	V1	Unknown	

### POLICY

COTA Victoria will provide the necessary information technology and telecommunication resources to efficiently undertake its mission and deliver on strategic plans. COTA Victoria will ensure all necessary technology is purchased and allocated in order to achieve optimal operational efficiency across the organisation.

When utilising technology, COTA Victoria will provide clear guidelines to the staff regarding appropriate conduct and behaviour. This includes the use of online/social networking and collaborative platforms. These individual interactions represent a new model: not mass communications, but masses of communicators. Through these interactions, COTA Victoria's greatest asset – the expertise of its employees – can be shared with members, stakeholders, and the communities in which it operates.

This policy covers all COTA Vic employees, including contractors and volunteers. All staff and volunteers are expected to comply with these procedures at all times to protect the privacy, confidentiality, and interests of our company, our services and our employees.

### PROCEDURES

#### Annual IT&T Plan

An annual IT&T plan will be developed that supports the delivery of the annual business and other functional plans. The plan will address functional process requirements and workforce composition. The plan will address operator competence requirements to ensure usage is efficient.

The plan will also identify resource and budgetary requirements to effectively and efficiently deliver the IT&T function.

The IT&T plan will then be used as an iterative process to assist COTA determine the feasibility of the business and functional plans.

Annual IT&T plans will test capacity in terms of type of equipment required by each role and project, quantity and availability, storage, Server and internet data transfer volumes and speed, print speeds, need for colour and mono printing.

Capacity will also be relevant to COTA's workforce schedules to facilitate shared equipment usage wherever economically sensible.

### **Purchasing Hardware/Software**

Any requests for new hardware or software must be directed through to the Manager – Organisational Support who will ensure they are compatible with the current system and at a specification that is consistent with the network and within budget. All hardware and software are registered either within the Asset Management Register or Software License Register.

### **Individual Computers**

Staff will be allocated access to programs from an allocated computer. As part of the induction process, Managers will direct staff to the appropriate drives, folders and printers to access. Managers will also provide staff with training on the Business Classification System for storage of documents. Any issues with access or programs should be raised to a Manager first, prior to completing the IT Support process.

### **Bring our Own Computer**

Guidelines are provided to staff and volunteers for the use of personally owned notebooks, smart phones and tablets for business purposes. All staff and volunteers who use or access COTA Victoria technology equipment and/or services are bound by this policy and the COTA IT Agreement. All personally owned devices must be approved for use by Management and registered with the Manager – Organisational Support. When using a personal device staff and volunteers must:

- Not download or transfer business or personal sensitive information to the device, for example intellectual property, client or staff/volunteer information.
- Not to use a registered mobile device as the sole repository for COTA Victoria's information;
- All business information stored on mobile devices should be backed up.
- Make every reasonable effort to ensure that COTA Victoria's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected.
- Maintain the device.
- Not to share the device with other individuals to protect the business data access through the device.
- To abide by COTA Victoria's internet use for appropriate use and access of internet sites etc.

- To notify COTA Victoria immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an untrusted or unknown source to COTA Victoria's equipment.

All employees and volunteers who have a registered personal mobile device for business use acknowledge that COTA Victoria:

- Owns all intellectual property created on the device;
- Will regularly back-up data held on the device;
- Will delete all data held on the device;
- Will delete all data held on the device upon termination of the employee. The terminated employee/volunteer can request personal data be reinstated from back up data.

### Accountability

Individual operators are accountable for the care (including cleaning) of assets they operate. This includes notifying the Manager – Organisational Support when maintenance is required.

### Usage

IT&T assets are provided for the purpose of meeting organisational needs. However, some incidental personal use is allowed where said use does not interrupt organisational needs.

All use of IT&T assets, including the internet, must be consistent with a professional office environment. A **conservative approach** must be taken to ensure no offensive, discriminatory or unprofessional material, content or activities occur. Transmission or viewing of sexually explicit material will result in disciplinary proceedings and may result in dismissal.

COTA will make IT&T access available for work from home purposes as an exception, which is approved on a case by case basis by their Manager.

Individuals are responsible for ensuring their use of COTA IT&T resources does not result in a breach of privacy or copyright legislation.

### Electronic Purchasing

All electronic purchases by any authorised employee must adhere to the COTA Victoria Procurement and Purchasing policies.

Where an electronic purchase is being considered, the person authorising this transaction must ensure that the internet sales site is secure and safe and be able to demonstrate that this has been reviewed.

All electronic purchases must be undertaken using business credit cards only (unless authorisation is provided by Management) and therefore adhere to the COTA Victoria Credit Card Policy.

### Training

Asset training needs will be addressed prior to operating IT&T assets. Training needs will also be addressed based on the consolidated help desk incident log.

## Passwords

All passwords must have a minimum of 8 characters and contain a minimum of:

- One (1) Uppercase character
- One (1) Lowercase character
- One (1) Number
- One (1) Character sign, eg \* @ #

Passwords are automatically reset bi-annually in September and March of each year and must not be altered without the permission from the Manager, Organisational Support. All passwords are held confidentially in a safe area with the Manager – Organisational Support.

Passwords are not to be shared and remain private and confidential with the exception of the CEO, Manager and Manager - Organisational Support.

## Network

The COTA Victoria network is set up to allow access from either direct input or via remote access, which can be arranged for authorised staff.

The commencement of a new staff member requires notification to the Manager, Organisational Support in order to have network access and specialist programs allocated.

## Email

E-mail is a vital tool for the conduct of COTA Victoria business. Upon commencement at COTA Victoria each employee will be given an e-mail address, generally the staff members initial and surname ([jsmith@cotavic.org.au](mailto:jsmith@cotavic.org.au)) or ([jjones@seniorsrights.org.au](mailto:jjones@seniorsrights.org.au)) is used for the beginning of the address and then @cotavic.org.au or @seniorsrights.org.au. Email signatures are determined by the organisation and should not be varied by individual staff.

The provision of e-mail is essential for the conduct of COTA Victoria's business and as such users need to be aware that management of the organisation reserves the right to access any individuals e-mail at any time. COTA email addresses should not be used for personal use. Minor personal use of email using a personal email address is allowed, assuming the use does not interrupt organisational needs.

Using a COTA email to distribute offensive or pornographic material or chain letters is strictly forbidden. Any email received from an unknown source or that looks "suspicious" should be deleted immediately from both email and rubbish box and the Manager, Organisational Support, notified. Do not forward the email.

## Internet

Internet connection is available on all computer desktops as it is essential for the conduct of COTA Victoria's business. Staff are expected to utilise this for the conduct of their work. COTA Victoria reserves the right to audit sites visited by staff.

Minor personal use of the internet is allowed, assuming the use does not interrupt organisational needs. Accessing pornography or other offensive material or engaging in non-work related discussion or chat groups is strictly forbidden and if detected may result in disciplinary action or dismissal.

### **Software**

COTA VICTORIA has a standard operating environment on all computers and an audit is regularly undertaken on all software on all computers. It is important that staff or volunteers do not introduce any outside software without written approval from the Management, regardless of its cost. For additional software purchases, a request for the purchase must proceed through to the Manager and will be considered within the normal budgetary context.

### **Licences**

All software purchased or downloaded by COTA Victoria, carries a licence which is a legal contract between the supplier and purchaser. It is an offence by law to use any software that has not been licenced to COTA Victoria or is unlicensed on a COTA Victoria computer. The use of this software carries significant penalties and will be dealt with seriously.

### **Saving Work**

Staff should save work on a regular basis (with the default setting – 5 minutes) during the normal day and make sure all work is saved before closing down the computer. All staff should be aware that the CEO or nominee has complete access to the system. Staff should also be aware that from time to time the Manager – Organisational Support may have complete access, however, will only access information under the authority of the CEO or for the purposes of managing COTA's IT.

### **Backup of Work**

Responsibility for ensuring that a backup is completed regularly is the Manager – Organisational Support. Backup is carried out on a regular basis; this ensures that in the case of equipment failure, the information loss is limited. All data should be stored on your designated drive on the server as the server is backed up not the individual computer hard drive.

### **Virus Protection**

All COTA Victoria computers have up-to-date virus protection, spam identification and protection cover that in conjunction with the internet service provider, provides extensive protection to the system. However, minimal spam does manage to enter the system. If this occurs, the user should enable "mail guard" by clicking the spam removal message at the bottom of the spam email.

### **IT Support**

When assistance is required, the following steps should be undertaken.

1. Remove and reconnect all power and blue network cables
2. Ensure remaining cords are connected
3. Shut down the computer in its entirety and turn back on

Should this not resolve the issue, report the problem to the Manager – Organisational Support following these steps:

1. Email [it@cotavic.org.au](mailto:it@cotavic.org.au)
2. Within the email message, answer the following questions:
  - What is the priority of the issue (staff can refer to below - Help Desk levels 1-4 for ideas);
  - What is the piece of equipment/software?
  - What seems to be happening/problem?
  - How long has this been occurring?
  - What have you tried?
  - Provide any images of screen messages of errors.
3. A return email will acknowledge the receipt

The Manager – Organisational Support will triage the requests and develop a strategy for addressing them. This includes the possibility of involving other staff members who have the skill set required to resolve the issue. Alternatively a third party provider could be contacted for assistance. In the absence of the Manager – Organisational Support and where the matter is urgent, staff are to consult with their Manager who has the responsibility to contact the IT Service Provider to rectify the issue. Staff should not contact the IT provider direct as this incurs a cost to the organisation which needs to be approved by the Manager.

### Help Desk

A help desk function will track all incidents and issues, system and operator failures, as an input to the IT&T annual plan and ongoing corrective measures. Incident log will segment the nature of the problem under hardware, software, capacity and operator competence. Severity of incidents will be segmented into priority levels with defined corrective timelines to ensure corrective action and limited resources are focused on the highest business need.

- **Level 1 mission critical** – COTA is unable to carry out its stated mission on a broad scale, response will be within three hours.
- **Level 2 high business priority** – the issue is having a major impact on COTA's operations, response will be within working 8 hours.
- **Level 3 important** – issue is affecting more than one staff member or a major project timeline, response will be within 24 working hours.
- **Level 4 moderate to low impact** – issue is affecting a small number of staff and they can undertake alternate duties while problem is being resolved, within 2 working days.

Where there is failure of any of the business's hardware, this must be referred to Manager – Organisational Support or in their absence, George Petrovic from Prompt Networks immediately.

It is the responsibility of Manager – Organisational Support to undertake tests on planned emergency procedures, quarterly, to ensure that all planned emergency procedures are appropriate and minimise disruption to business operations.

### **Emergency Management**

#### **Point of Sale Disruptions**

In the event that point of sale system is disrupted, the following actions must be immediately undertaken:

- POS provider to be notified
- Senior Bookkeeper must be notified immediately
- All POS transactions to be taken using the manual machine
- For all manual POS transactions, customer signatures must be verified

#### **Virus or other security breach**

In the event that COTA's information technology is compromised by software virus such breaches are to be reported to Manager – Organisational Support immediately.

The Manager – Organisational Support is responsible for ensuring that any security breach is dealt with to minimise disruption to business operations.

#### **Website Disruption**

In the event that COTA's website is disrupted, the following actions must be immediately undertaken:

- Website host to be notified
- Marketing & Communications Advisor and Manager – Organisational Support must be notified immediately

### **RELEVANT DOCUMENTS & FORMS**

---