	<b>ADRA Australia Policies and Procedures</b>		<b>No. CS 190 100</b>
	<b>Document Name</b>		<b>Page 1 of 11</b>
	Acceptable Information Technology Usage		
	<b>Department</b>	<b>Sections</b> (inc. All sections where this document is located.)	
	Corporate Services	Corporate Services	
	<b>Modified By</b>	<b>Document Version</b>	<b>Effective Date</b>
	SPD ACTS/Maddocks	2017/1.1	5 September 2017
<b>Approving Committee</b>	<b>Previous</b>	<b>Revision Date</b>	
ADRA Board of Directors		2019	



*This policy applies to both ADRA Australia and Open Heart International. Unless specifically mentioned in the policy, references to ADRA Australia extend to, and include, Open Heart International.*

## CS 190 100 Acceptable Information Technology Usage

### 1. PURPOSE AND SCOPE

In relation to information technology usage this policy sets out expectations for the behaviour and standards of professional and personal conduct for ADRA Australia’s employees (including Conference ADRA Directors), volunteers, contractors and Company Directors hereinafter referred to as ADRA Australia Personnel in their engagement with ADRA Australia.

This policy is sourced from the Seventh-day Adventist Church Technology Services in the South Pacific Division and as such may be updated at their discretion from time to time. It is the responsibility of each user to have read and understood this policy as a condition of access.

Access and computing privileges are accompanied by responsibilities to use corporate computing resources in an ethical, legal and efficient manner, consistent with the mission, ideals, and corporate directives of ADRA Australia and the Seventh-day Adventist Church and with the purpose for which such resources are intended. Every user is responsible to:

- abide by this policy
- report suspected breaches
- report any unauthorised use made of accounts, usernames, or passwords

### 2. SECURITY


#### A. PASSWORDS

The use of your computer, including access to email and other corporate resources, is controlled by the username assigned to you by your IT support staff, and the password you choose and manage. Passwords shall be complex (they shall include at least 1 number and 1 character) and changed every 90 days. Users must not use a username/password assigned to another user without the approval of their IT Manager.

Users will be held responsible for all activities, including email, internet and network access made using their username and password. Users must not divulge passwords to individuals other than IT Support. Users should not leave computers unattended while logged in. It is recommended computers be locked (Windows Key + L) when left unattended.

#### B. ASSETS

No computing equipment assets shall be removed from employer property without the explicit written permission of the IT Manager/Supervisor, other than laptop computers which can be utilised by authorised laptop computer users, peripherals and projectors. Please note; use of equipment in a way that is outside of this policy could result in personal responsibility for any subsequent loss or damage.

	<b>ADRA Australia Policies and Procedures</b>		<b>No. CS 190 100</b>
	<b>Document Name</b>		<b>Page 2 of 11</b>
	Acceptable Information Technology Usage		
	<b>Department</b>	<b>Sections</b> (inc. All sections where this document is located.)	
	Corporate Services	Corporate Services	
	<b>Modified By</b>	<b>Document Version</b>	<b>Effective Date</b>
	SPD ACTS/Maddocks	2017/1.1	5 September 2017
<b>Approving Committee</b>	<b>Previous</b>	<b>Revision Date</b>	
ADRA Board of Directors		2019	



*This policy applies to both ADRA Australia and Open Heart International. Unless specifically mentioned in the policy, references to ADRA Australia extend to, and include, Open Heart International.*

All computer hardware assets shall be recorded in a spreadsheet or database including an accurate description, purchase date, serial number, warranty expiry date, and the person that the hardware is assigned to or the physical location of that asset, and the date the asset should be returned and considered for replacement.

All computer hardware assets assigned to staff, should include a matching form outlining dates that the equipment was checked out, and when it is to be returned. This covers short term loan for equipment such as projectors, and longer term such as personally assigned laptops, and this form should include relevant information about due care and potential personal liability for damage or loss. Laptops are vulnerable to theft, damage or loss, and unauthorised access. Extra care should be taken to safeguard and backup sensitive corporate information.

- Never leave your laptop in your vehicle overnight.
- If it is unavoidable to leave your laptop in your unattended vehicle for short periods during your working day, lock it in the boot, & ensure the laptop is secured out of sight.
- When travelling by air, take your laptop as cabin baggage. Do not check it in to the hold, as your insurance cover will not apply to loss or damage incurred as checked in baggage regardless of whether or not it is packed inside a checked suitcase.
- Do not leave your laptop unattended in a public place at any time.

### C. NETWORK


Devices which can be connected to the external internet or networks such as personal wireless access points, storage devices that can be connected to by other computers, or any other devices which other computers can connect to, shall not be connected to or used from desktops, laptops or other computer assets while these devices are simultaneously connected to the network. Network-capable devices (other than authorised corporate desktops or laptops, or approved wireless access solutions) shall not be physically connected to the network (either directly or indirectly) without prior authorisation by the relevant IT Manager / IT Supervisor. This includes, but is not limited to:

- Personally owned computing equipment, including laptops and desktops
- ADSL or wireless modems
- Any form of public internet connection beyond those provided
- Wireless access points of any kind (including external wireless Hard-drives).

## 3. HARDWARE AND SOFTWARE

### A. ACQUISITION

Check with the local IT Manager/ IT Supervisor for authorisation before purchasing any software or computer related equipment that may be connected to ISG network equipment that it complies with hardware and software standards. Unauthorised software may be removed without notice by local IT staff or ISG IT staff, where it impacts computer or network stability, or is believed to cause any disruption or threat. All software and hardware purchases must be approved in accordance with the IT hardware and software standards policies. Any software or stored files which are not legal or are

	<b>ADRA Australia Policies and Procedures</b>		<b>No. CS 190 100</b>
	<b>Document Name</b>		<b>Page 3 of 11</b>
	Acceptable Information Technology Usage		
	<b>Department</b>	<b>Sections</b> (inc. All sections where this document is located.)	
	Corporate Services	Corporate Services	
	<b>Modified By</b>	<b>Document Version</b>	<b>Effective Date</b>
	SPD ACTS/Maddocks	2017/1.1	5 September 2017
<b>Approving Committee</b>	<b>Previous</b>	<b>Revision Date</b>	
ADRA Board of Directors		2019	



*This policy applies to both ADRA Australia and Open Heart International. Unless specifically mentioned in the policy, references to ADRA Australia extend to, and include, Open Heart International.*

not approved may be removed and local user security may be reduced down from administrative rights.

## **B. COPYRIGHT AND LICENSING**

Two situations regarding software procurement and licensing include system wide software, and local entity needs. In the case of software centrally managed within ISG, installation is executed by ISG staff, or under their authority. This includes antivirus and network components (security, email, remote desktop) for all software such as office tools/readers and desktop publishing tools. Please refer to your local IT support personnel for procurement and installation.

All employees shall abide by software copyright laws and shall not obtain, install, replicate, or use software except as permitted by the software licensing agreements. No unlicensed software is to be installed on any computing resource and action to rectify a detected breach will be taken by an IT staff member. Any fines and costs incurred as a result of the use of or saving of unlicensed software shall be the responsibility of the user. Users may have conditions placed on their computing access by the employer or principal at any.

## **C. NON-CORPORATE SOFTWARE**

In order to protect the integrity of local IT computing resources, employees shall not use personally-owned software on such resources, without prior consultation with and approval from their IT manager / IT supervisor. This includes purchased and licensed applications; shareware; freeware; downloads from bulletin boards, Internet, Intranet, FTP sites, local area networks or wide area networks; and other personally-owned or controlled software.


## **4. COMMUNICATIONS, EMAIL & MESSAGING**

### **A. ACQUISITION**

Communications, Email and Messaging in this document refers to the all technology and systems employed by the organisation to enable communication between people and groups with the aid of employer provided equipment, or any equipment connected to employer provide networks or services. This includes, but is not limited to, the following facilities:

- The corporate email system and email tools
- Other systems and applications with messaging capabilities (e.g. web-based email systems, social networking and blogs)
- Printers, photocopiers, scanners and facsimiles
- Telephones, recording devices
- Any other tools for communication as part of employment purposes

Email and all relevant forms of communication may be monitored and reviewed, and employees using corporate resources for the transmission or receipt of communications shall have no expectation of privacy. Email communications records are official documents and subject to the

	<b>ADRA Australia Policies and Procedures</b>		<b>No. CS 190 100</b>
	<b>Document Name</b>		<b>Page 4 of 11</b>
	Acceptable Information Technology Usage		
	<b>Department</b>	<b>Sections</b> (inc. All sections where this document is located.)	
	Corporate Services	Corporate Services	
	<b>Modified By</b>	<b>Document Version</b>	<b>Effective Date</b>
	SPD ACTS/Maddocks	2017/1.1	5 September 2017
<b>Approving Committee</b>	<b>Previous</b>	<b>Revision Date</b>	
ADRA Board of Directors		2019	



*This policy applies to both ADRA Australia and Open Heart International. Unless specifically mentioned in the policy, references to ADRA Australia extend to, and include, Open Heart International.*

same laws as other forms of correspondence. As such they can be subpoenaed or discovered during legal processes.

Access to corporate email systems is provided for employees whose duties require email to fulfil their responsibilities. All users should maintain a separate personal email address (such as one of the many free webmail services like gmail, hotmail, and yahoo), for any personal email, rather than their corporate account. These web based mail and chat services can be made accessible from employer provided facilities at the discretion of the employer, for reasonable levels of personal usage during work hours if it does not interfere with work responsibilities and if it does not impact or degrade any IT services. Such personal usage may be subject to the same scrutiny for ensuring the same acceptable usage where any such communications are being transmitted from employer facilities (and hence may be recorded and traced back to employer owned facilities).

#### **B. ACCEPTABLE USAGE**

Employer email facilities are provided to facilitate the conduct of corporate business, and any usage is to conform to this policy. Any usage should not be used in any way which interferes with computing resources and facilities, or impacts the ability of any employees to execute their duties.


#### **C. MANAGEMENT OF INAPPROPRIATE EMAIL**

If you receive an inappropriate email you must inform the person distributing the email that it is against the Church's policy for you to receive this type of material. If the email was sent to you as a member of a distribution list, you must also request to be taken off the distribution list. If you unknowingly open an inappropriate email, you must delete the message without opening any attachments. You must not distribute the message to colleagues and must not save the message or attachments. You must not purport to agree to anything on your employing organisation's behalf unless you are authorised in writing to enter into such an agreement. All such emails you send should be accurate and complete.

#### **D. PROHIBITED USES OF EMAIL**

Prohibited use of email includes (but is not limited to) sending or arranging to receive:

- chain letters (forwarded human interest emails, or ideas), or any unauthorised mass mailings
- information that violates state or federal laws, or Church policies
- unsolicited commercial announcements or advertising material
- personal business of the employee for advertising or conducting business
- general interest or fund raising solicitation to any office or group email distribution lists, with the exclusion of mission or outreach projects that have been adopted and approved by administration for transmission within that relevant local institution or entity only
- any material that may defame, harass, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, your employing organisation or the Church, the recipient, the sender, or any other person
- pornographic, racist or offensive images or material
- malicious code
- unauthorised information including anything that is sensitive, confidential, proprietary,

	<b>ADRA Australia Policies and Procedures</b>		<b>No. CS 190 100</b>
	<b>Document Name</b>		<b>Page 5 of 11</b>
	Acceptable Information Technology Usage		
	<b>Department</b>	<b>Sections</b> (inc. All sections where this document is located.)	
	Corporate Services	Corporate Services	
	<b>Modified By</b>	<b>Document Version</b>	<b>Effective Date</b>
	SPD ACTS/Maddocks	2017/1.1	5 September 2017
<b>Approving Committee</b>	<b>Previous</b>	<b>Revision Date</b>	
ADRA Board of Directors		2019	



*This policy applies to both ADRA Australia and Open Heart International. Unless specifically mentioned in the policy, references to ADRA Australia extend to, and include, Open Heart International.*

including but not limited to financial data, personnel records, tendering and pricing information and contracts, internal memos, minutes of meetings, management reports or business operation details, emails that were not intended for the new recipient and any information for which distribution is not authorised for employment and organisational purposes

- software, music, pictures or any files or resources that are protected by license or copyright, unless you know that transmitting it is lawful both at the source and destination
- large attachments to bulk mailing lists, or any attachments that are not work related.

#### **E. EMAIL SIZES**

Email systems are not designed to transfer large files. When attached to messages, such files overload network links, degrading the performance of the email system, inconveniencing users who may be on slow links and disrupting work flow. Emails with large attachments should not be sent to bulk mailing addresses internally. Alternatives exist for the transfer of very large files contact your local IT person if you need assistance with this. For bulk internal lists any attachment over 150k would be considered unreasonably large for distribution to all office users, or bulk mailing list, with the exclusion of images, documents, spreadsheets, or resources which are directly work related and which cannot be share by network and which must be copied to a specific group or people.

Maximum message sizes (message + attachments) outside of the scenarios covered already have been set at 10MB for outgoing email and 10MB for incoming internet email, and these limits may be changed to meet with changing needs and conditions. Note that many companies have email limits below these current limits, attempts to send large attachments may still be rejected by these mail servers even though they fall within our limits.



#### **F. VIRUSES**

Virus activity is a continually evolving threat to the reliability of our computing equipment and services. To counter these threats virus checking and removal software must be activated on all machines and must not be turned off by the user. Electronic material obtained from third parties or from the Internet may contain viruses or similar destructive agents. Users should not open attachments from an unknown source without taking appropriate methods to test the authenticity and to ensure any such item is free of viruses or other malicious code. When in doubt, please contact your local IT person rather than to leave things to chance. In any event that a user knowingly tampers with or disables anti-virus, disciplinary action may be undertaken. It may result in a reduction in user security levels or complete removal of computing privileges.

#### **G. EMAIL ACCESS**

Even if the employee is contactable and able to access their email, the employee may delegate access or request access be delegated to certain approved personnel. An employee's supervisor may also request access to an employee's email at any time.

### **5. INTERNET**

	<b>ADRA Australia Policies and Procedures</b>	<b>No. CS 190 100</b>		
	<b>Document Name</b>	<b>Page 6 of 11</b>		
	Acceptable Information Technology Usage			
	<b>Department</b>	<b>Sections</b> (inc. All sections where this document is located.)		
	Corporate Services	Corporate Services		
	<b>Modified By</b>	<b>Document Version</b>		<b>Effective Date</b>
	SPD ACTS/Maddocks	2017/1.1		5 September 2017
<b>Approving Committee</b>	<b>Previous</b>	<b>Revision Date</b>		
ADRA Board of Directors		2019		

*This policy applies to both ADRA Australia and Open Heart International. Unless specifically mentioned in the policy, references to ADRA Australia extend to, and include, Open Heart International.*

## A. ACQUISITION

Internet access is available to employees and contractors whose duties require it for the conduct of corporate business from corporate computing equipment. Since Internet activities may be monitored, all personnel accessing the Internet shall have no expectation of privacy. Access to the Internet is via a firewall and web filters for computers connected directly to the corporate network, and these should not be bypassed without express approval from IT management.

## B. ACCEPTABLE USE

The employer provides Internet access to facilitate the conduct of corporate business. Any usage must not interfere with the work of other personnel or IT staff ability to perform their function, and all usage must be consistent with official corporate directives. All users must comply with state and federal laws. See Appendix A for current restrictions and filters applied to internet usage. This is not an exhaustive list and can change from time to time. Any exclusions to this would be by request and approval case by case, where such usage is demonstrated as a necessary part of one's employment.



## C. PROHIBITED USE

Prohibited activities when using the Internet include (but are not limited to):

- Browsing pornographic, offensive or hate-based web sites, hacker or cracker sites, online gambling sites, or sites connected with illegal activities of any kind.
- Posting, sending, or acquiring sexually explicit or sexually oriented material, hate-based material, hacker-related material, illegal material of any kind, or other material inconsistent with the Seventh-day Adventist corporate ideals and objectives.
- Posting or sending sensitive information outside without management authorisation.
- Promoting or maintaining a personal or private business.
- Browsing social networking sites and dating sites for personal purposes.
- Using non-work related applications or software that uses Internet bandwidth continually for unauthorised and un-work-related interests (e.g. webshot-style screensavers, file-sharing applications, streaming audio and or video).
- Activities that circumvent or compromise network and computer security controls.
- Unauthorised use of any Internet service, including systems for which the user does not have an authorised account.
- Use of any internet service that is inconsistent with the lifestyle and values fitting a member of the Seventh-day Adventist church.
- Accessing any material that you have no authorisation to access.
- Sending material that you have no authorisation to send.

## 6. NETWORK STORAGE USAGE POLICY

### A. BUSINESS DATA FILES

	<b>ADRA Australia Policies and Procedures</b>	<b>No. CS 190 100</b>		
	<b>Document Name</b>	<b>Page 7 of 11</b>		
	Acceptable Information Technology Usage			
	<b>Department</b>	<b>Sections</b> (inc. All sections where this document is located.)		
	Corporate Services	Corporate Services		
	<b>Modified By</b>	<b>Document Version</b>		<b>Effective Date</b>
	SPD ACTS/Maddocks	2017/1.1		5 September 2017
<b>Approving Committee</b>	<b>Previous</b>	<b>Revision Date</b>		
ADRA Board of Directors		2019		

*This policy applies to both ADRA Australia and Open Heart International. Unless specifically mentioned in the policy, references to ADRA Australia extend to, and include, Open Heart International.*

Network storage primarily exists for storing business documents, spreadsheets, and records that have some form of reference value or legal requirement for the future. Quotas set by agreement will be enforced on these drives. The following are descriptions of files that are considered appropriate business:

- Spreadsheets with business related information such as financial reports, budgets, expense reports, etc
- Documents with business related information, procedures, policy, agreements, contracts, constitutions etc
- PDF files specifically of contracts / business related content, should have minimal graphics
- Any other file types which contain information of a similarly important business nature

## **B. RESOURCE FILES**

Resources for departmental, office, or broader shared access must be contained within appropriately assigned quotas. This is principally intended for files that have a current or future purpose. This would include the following broad categories:

- Presentations (sermons, illustrations, training materials, etc)
- Audio and/or Visual resources (where these are materials / resources that have relevance to other personnel for which copy is a legal right)

## **C. PERSONAL DATA FILES - MANAGED BY INDIVIDUAL**

At no time should personal files be backed up to network locations, except by permission with the Service Desk and/or the local site IT manager for temporary purposes. As laptops are permitted to be used for personal purposes local HDD's on laptops may contain various personal files such as photos and personal banking and finance, as well as personal music or other files to the extent where it does not impact on the work responsibilities of the user on that laptop. Personal resources includes photos from a trip, or interesting resources that may be used in creating sermons, illustrations, etc. Backing up all of these files is the responsibility of the user. Users are encouraged to back up personal files on their own independent storage devices.


Personal files if detected on the network may be removed, particularly where this is necessary to resolve space problems, or if necessary to resolve network performance impacts relating to file replication and backup processes. These may be detected through review of files lists by size, on the basis of folder and filenames, and anything which seems to be of a personal nature may be accessed to determine its relevance.

## **D. PROHIBITED USES OF LOCAL AND NETWORK STORAGE**

In regard to any materials that are saved on network storage to which copyright exists, there must be a basic text file or document saved in the same directory, with sufficient reference information or evidence of ownership or rights to retain the copy on a network drive.

All the following categories represent files that are inappropriate for storage on network drives or local computers at any time:

- Any music, graphics, software or other file formats or resources that are in breach of

	<b>ADRA Australia Policies and Procedures</b>		<b>No. CS 190 100</b>
	<b>Document Name</b>		<b>Page 8 of 11</b>
	Acceptable Information Technology Usage		
	<b>Department</b>	<b>Sections</b> (inc. All sections where this document is located.)	
	Corporate Services	Corporate Services	
	<b>Modified By</b>	<b>Document Version</b>	<b>Effective Date</b>
	SPD ACTS/Maddocks	2017/1.1	5 September 2017
<b>Approving Committee</b>	<b>Previous</b>	<b>Revision Date</b>	
ADRA Board of Directors		2019	



*This policy applies to both ADRA Australia and Open Heart International. Unless specifically mentioned in the policy, references to ADRA Australia extend to, and include, Open Heart International.*

copyright

- Any materials that are not in harmony with the morals and teachings of the Adventist church
- Any materials which are in breach of any workplace legislation or church working policy, including copyright or privacy

The following categories represent files that should not be stored on the corporate network, generally T: or S: drive):

- Personal files of any type, including personal finances, photos, etc
- Backups of local computers / files
- Any resources that are individual by nature and do not need to be shared within the department, and would not remain with the organisation if the individual was to move to another role / location

## 7. GENERALLY PROHIBITED USE OF COMPUTING RESOURCES

### A. ILLEGAL ACTIVITY

Generally prohibited activities when using organisation provided computing resources (hardware, software, networks, applications) shall include:



- Stealing, copying or keeping of electronic files without permission
- Violating copyright laws
- Writing, copying, executing, or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any corporate computer, network, or information
- Conducting fraudulent or illegal activities, including but not limited to: gambling, trafficking in drugs or weapons, participating in terrorist acts, threats to national security, or attempting unauthorised entry to any corporate or non-corporate computer or network
- Creating, sending or accessing any material which may discriminate against, harass or vilify colleagues or any member of the public, or any group of people based on sex, pregnancy, age, race (including colour), nationality, descent or ethnic background, religious background, marital status, disability, medical condition, and homosexuality or transgender status

### B. OTHER INAPPROPRIATE ACTIVITY

Other prohibited activities when using organisation provided computing resources (hardware, software, networks, applications) include:

- Browsing the private files or accounts of others, except as provided by appropriate authority
- Performing unofficial activities that degrade system performance, such as the playing of electronic games
- Performing activities intended to circumvent security or access controls, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, tunnelling, elevation or by-passing of access rights, or compromise information security by



	<b>ADRA Australia Policies and Procedures</b>	<b>No. CS 190 100</b>		
	<b>Document Name</b>	<b>Page 9 of 11</b>		
	Acceptable Information Technology Usage			
	<b>Department</b>	<b>Sections</b> (inc. All sections where this document is located.)		
	Corporate Services	Corporate Services		
	<b>Modified By</b>	<b>Document Version</b>		<b>Effective Date</b>
	SPD ACTS/Maddocks	2017/1.1		5 September 2017
<b>Approving Committee</b>	<b>Previous</b>	<b>Revision Date</b>		
ADRA Board of Directors		2019		

*This policy applies to both ADRA Australia and Open Heart International. Unless specifically mentioned in the policy, references to ADRA Australia extend to, and include, Open Heart International.*

any other means

- Promoting or maintaining a personal or private business, or using corporate information resources for personal gain
- Conducting unauthorised fundraising, the unauthorised endorsement of any product or service, lobbying, or participating in any partisan political activity
- Creating, sending or accessing any information that could damage the Church's reputation, be misleading or deceptive, result in victimisation or harassment, lead to criminal penalty or civil liability, or be reasonably found to be offensive, obscene, threatening, abusive or defamatory, or not in keeping with the values of the SDA Church

## 8. INDIVIDUAL POLICY

### A. INDIVIDUAL PRIVACY

All personnel acknowledge as a condition of employment and condition of access to computing resources that all emails, internet usage logs, files, software and any information stored on employer provided computers or devices that connect to the organisation network are subject to monitoring by the organisation. This includes servicing any request at the direction of any person within the supervisory chain or administration for any of this information about a specific person. This also includes access by any IT administrators for monitoring and ensuring compliance with this policy

### B. PRIVACY LEGISLATION



The disclosure of any information beyond the specific requirements in this policy is forbidden, without the express written consent of the owner of that information. Under no circumstances should any information to which any user has access, be shared or distributed without authorisation by the Administration of the entity that is storing that information, within their own rights and obligations under current legislation.

All personnel also acknowledge that the Australian Government has privacy legislation, and all personnel are required to handle all personal details available to them in a manner consistent with the applicable legislation requirements.

### C. MONITORING

Monitoring may be random, periodic, or continuous, and may be done, among other things:

- To maintain effective management of computing resources;
- To assure compliance with IT policies
- To prevent inappropriate or excessive personal use of organisational property
- To investigate conduct that may be illegal, a breach of policy or adversely affect the organisation or its employees
- To provide information or direct access to the computer, email, or files, at the request of the relevant departmental head, director, or senior administrator, or supervisor within the line of authority

	<b>ADRA Australia Policies and Procedures</b>	<b>No. CS 190 100</b>		
	<b>Document Name</b>	<b>Page 10 of 11</b>		
	Acceptable Information Technology Usage			
	<b>Department</b>	<b>Sections</b> (inc. All sections where this document is located.)		
	Corporate Services	Corporate Services		
	<b>Modified By</b>	<b>Document Version</b>		<b>Effective Date</b>
	SPD ACTS/Maddocks	2017/1.1		5 September 2017
<b>Approving Committee</b>	<b>Previous</b>	<b>Revision Date</b>		
ADRA Board of Directors		2019		

*This policy applies to both ADRA Australia and Open Heart International. Unless specifically mentioned in the policy, references to ADRA Australia extend to, and include, Open Heart International.*

#### **D. INFORMATION WHICH MAY BE COLLECTED / AVAILABLE FOR MONITORING**

Information which may be collected/available for monitoring includes:

- Computer hardware and the employees to which the hardware is assigned including mobile device and tablets
- Software applications installed on computers.
- Hardware and system settings of computers.
- System access details, including but not limited to, logon attempts, file access and changes, file printing, and connections to server and network resources generally.
- Any resources (files of any type) saved onto any corporately owned computers or network drives
- Every web page requested, including but not limited to, address, date/time, and the username requesting the web page.
- Every email message sent and received, including but not limited to, the addresses of both the sender and receiver, the message size, and date/time sent/received, and the contents of all messages.

#### **E. BACKUP / AUDIT**

All email that is sent and received is immediately archived and available for future retrieval. The act of deleting any email will not remove it from email archival records. Any file or resource which is saved on network drives can be retrieved in the future where the backup copies existed inside normal backup timeframes. This backup window should cover at minimum yearly backups indefinitely, 12 months rolling monthly backups, 4 weeks rolling weekly backups and 5 business days nightly backups. Files excluded from this would include anything that is created and deleted within the same day, or similarly a file a couple of years old which was created and deleted in the same year, but not restored.


#### **F. DISCLOSURE**

Information compiled during investigation of a breach of this policy may be provided to an appropriate level of management, and such other persons or organisations they determine appropriate, for further action. The following IT employees have unrestricted direct access to the collected information detailed above: IT Manager, the IT Network Engineers and Senior IT Support Administrators

#### **9. VIOLATION OF POLICY**

Use of computing equipment or services suspected to be inconsistent with the requirements of this policy shall be monitored and maybe investigated. Monitoring occurs intermittently primarily on an exception basis when there is cause for investigation, but also such needs may be detected during general IT administration activities including but not limited to general review of items like total storage utilisation that reveal abnormal usages. Suspected breaches of any provisions in this policy may be investigated, and may result from the action including but not limited to the following at the discretion of the Employer:

- Further investigation
- Counselling

	<b>ADRA Australia Policies and Procedures</b>		<b>No. CS 190 100</b>
	<b>Document Name</b>		<b>Page 11 of 11</b>
	Acceptable Information Technology Usage		
	<b>Department</b>	<b>Sections</b> (inc. All sections where this document is located.)	
	Corporate Services	Corporate Services	
	<b>Modified By</b>	<b>Document Version</b>	<b>Effective Date</b>
	SPD ACTS/Maddocks	2017/1.1	5 September 2017
<b>Approving Committee</b>	<b>Previous</b>	<b>Revision Date</b>	
ADRA Board of Directors		2019	



*This policy applies to both ADRA Australia and Open Heart International. Unless specifically mentioned in the policy, references to ADRA Australia extend to, and include, Open Heart International.*

- Suspension of access to computing resources
- Suspension or termination of employment
- Legal action