Archdiocese of Hobart

Policy and Procedures

ICT COMPUTING AND COMMUNICATIONS USAGE POLICY		Document # AOH-IT001	Print Date N/A
		Prepared By: ICT Manager	Date Prepared: 10 November 2015
Effective Date: 25 February 2016	Revision # V8	Reviewed By: Compliance Officer	Date Reviewed: 10 February 2016
Compliance: Broadcasting Services Act 1992 (Commonwealth) Copyright Act 1914 (Commonwealth) Personal Protection Act 2004 (Tasmania) Privacy Act 1988 (Commonwealth) Tasmanian Police Offences Act 1937 Telecommunications Act 1997		Approved By: Business Manager	Date Approved: 21 February 2016

The final page of this Policy needs to be printed, signed and returned to HR & Compliance.

Purpose

The purpose of this policy is to ensure all Archdiocese of Hobart (Archdiocese) employees are aware of the proper and expected usage of electronic devices and media, the management of information and the storage of data within the Archdiocese and its Agencies. Each employee/staff member, volunteer or user of any such equipment or who has access to information within the Archdiocese of Hobart is to read and sign this policy as acceptance of the information and guidance contained herein.

Policy

The Archdiocese of Hobart (Archdiocese) provides its employees with access to computing equipment, systems, services, software and information for the undertaking of work related processes applicable to the job description/role of the employee. These services collectively known as Information, Communication and Technology (ICT), include all forms of digital data, access to internal and external networks and all forms of digital communication and use of media. Examples include: internet, email, storage and any form of digital communication (e.g. video, chat, voice recordings, web conferences, web sites etc.) which provided for work purposes and the realisation of the Archdiocese's Mission.

Other persons who are not employees may also have entitlements to use Archdiocese ICT services, information, equipment and media, providing their use is contributing to the Mission of the Archdiocese. The Archdiocese does not permit the use of these services for personal gain and other personal commercial endeavours.

The Archdiocese recognises the varied use to which ICT services may be put for business purposes but does not permit the use for any purpose that may contravene any State or Commonwealth law or regulation.

The Archdiocese does not permit the use of ICT services in a way that may give offence to any person, be they employees or volunteers of the Archdiocese or any person that may receive information or a communication generated through the use of computing equipment or electronic facilities.

Any use of ICT Services by employees/staff or volunteers contrary to this policy or the attached guidelines will be deemed to be a breach of the Workplace Behaviour Policy of the Archdiocese of Hobart and may result in disciplinary action up to and including termination of employment.

For the purpose of this Policy all employees/staff, volunteers and other persons that have access to the Archdiocesan ICT Services will be known as users.

This Policy lists the guidelines to be followed when using any ICT Services including usage of equipment, accessing and sharing information provided by the Archdiocese or its Agencies. A Glossary is listed at the end of this agreement.

An agreement statement located at the end of this document is to be signed by the user, confirming understanding and acceptance of the Policy.

Scope

This Policy applies to all employees, volunteers and other persons of the following agencies within, and at all of the sites of, the Archdiocese of Hobart. Whilst the overall intent is applicable to all agencies, specific procedures and policies only apply to Business Units and Agencies that are members of the ICT Archdiocesan network. This is currently known as the AOHTAS network. The use of the term Archdiocese throughout this Policy refers to the Archdiocese of Hobart and its Agencies.

- Office of the Archbishop
- Parishes
- CatholicCare Tasmania
- Centacare Evolve Housing
- Catholic Development Fund
- Church Office.

Guidelines

The Archdiocese provides employees/staff with ICT Infrastructure that includes provision of software, storage, computing devices, access to internal and external resources and services to assist and enable staff in the effective carriage of their work. In addition to enabling staff, important requirements of ICT infrastructure usage are security and compliance. Protection of Archdiocesan staff, intellectual property, information and equipment is important for the effective and safe operations of Archdiocesan work and meeting the Mission of the Archdiocese. These guidelines are to assist all users of the Archdiocesan ICT network.

1. Use and Security of Computing Devices

1.1 All computing and electronic equipment is provided for work purposes.

1.2 All employees/staff, volunteers and other persons are not to use Archdiocese computing/electronic resources or facilities for personal gain and other personal commercial endeavours.

1.3 Contractors are not to use Archdiocese computing devices unless a contractual arrangement has been signed and a relevant computer user account has been created.

1.4 Computing devices issued to staff are to be kept secure and are not permitted to be used by family members or other unauthorised personnel.

1.5 All computing and electronic equipment is to be treated with due care and is to be kept in proper working order. Wilful damage to equipment may result in disciplinary action.

1.6 Any faulty or damaged computer equipment is to be immediately reported to ICT Services.

1.7 Any theft or loss of equipment is to be immediately advised to ICT Services to ensure continued security of the Archdiocese systems.

1.8 Other than mobile devices; no computer device, peripheral or software is to be removed from the workplace without prior written approval by the ICT Manager.

1.9 No work device including smart phones are to be taken or used internationally without the written permission of the Business Manager, the appropriate Corporate Services Units advised, the work device configured appropriately and the staff member advised of any financial accountability and security responsibilities. This is to minimise risk to Archdiocesan data/information and protect the staff member.

1.10 When on annual leave staff other than Managers or similar level, are required to keep their workstations at the workplace. This includes laptops, tablets or similar work devices. This rule excludes smart phones.

1.11 An exception to clause 1.10 above is provided by the staff member's Manager sending a written advice to ICT Services in advance of the leave period. The advice is to contain the staff member's name, equipment name and type taken off site, and dates of leave.

1.12 ICT Support for staff that have taken equipment interstate or on leave without prior arrangement with ICT Services will be based on 'best effort'.

1.13 Custodians of mobile devices are responsible for the safe keeping of their equipment either at work premises or offsite.

1.14 Archdiocesan workstations are supplied for business purposes and are configured to operate within the Archdiocesan network to minimise risk to users.

1.15 All Users of Archdiocese issued equipment are to familiarise themselves with how to use the basics of their system, including antivirus scans, use of peripherals and checking basic operations and connectivity of their system. This is to be part of their induction and a requirement of their computer usage.

1.16 Any issues with computer equipment, software or connectivity to the Archdiocese network is to be reported to ICT Services as soon as possible.

1.17 All workstations including monitors are to be shutdown at close of business, unless otherwise advised by ICT technical staff.

1.18 A separate user account is to be created for volunteer computer usage. ICT Services is to be advised of the computer to be used and the access required prior to creating the volunteer account.

1.19 No volunteer or contractor is to logon to a staff member's computer using the staff member's logon credentials.

1.20 Users leaving their workstations unattended must lock their computer screens.

1.21 In a shared workstation environment (Hot Desk) Users must log off the system when finished using the workstation or when they will be away for a period of time. This is to ensure the workstation is available for use by other nominated staff or volunteers.

1.22 Should a work area require shared access using a generic login then the Area Manager is to seek approval from the ICT Manager, advising of the reasoning in writing

1.23 Users are not to use other Users' logon credentials, without expressed authority, to access any computing device, whether owned by the Archdiocese of Hobart or by any other organisation. Under the TASMANIAN POLICE OFFENCES ACT 1935 - SECT 43C this behaviour may be deemed illegal.

1.24 A User found attempting to access or actually accessing another User's credentials to gain unauthorised access to the system or Internet services without proper authorisation, may be subject to disciplinary action.

1.25 Complex passwords are required for compliance and security to access the Archdiocesan computing network. These features are integrated within Archdiocese ICT systems. Passwords are to consist of character symbols, alphanumeric character in upper and lower case. Passwords are to be a minimum of ten (10) characters in length unless otherwise specified by the ICT Manager.

1.26 The system prompts Users to change their passwords every quarter (90) days. New passwords are to be generated and the system disallows reuse of the previous five (5) passwords.

1.27 Users are responsible for keeping their passwords secure as they will be accountable for work or actions taken on any computing or mobile device using their login credentials.

1.27.1 Passwords are to be kept in a secure location

1.27.2 Users are not to share their password or access credentials with other persons

1.27.3 Users are permitted to advise ICT Services of their passwords for setup of equipment and troubleshooting purposes. The password must then be changed.

1.28 Security codes will and are to be used to access mobile devices and apps that link to Archdiocesan data and information.

1.28.1 Security Codes issued for smart phone access are not to be altered unless ICT Services is advised in writing.

1.29 Data encryption is mandatory on all portable workstations with Direct Access enabled.

1.30 Users issued with Direct Access portable workstations are to enter the assigned Bit locker code for that workstation to access the device. This is a five digit numeric code.

2. Information Use and Access of Resource

2.1 The Archdiocese has the right to monitor and audit computer and staff usage of emails, internet and storage devices to manage and protect the integrity of the Archdiocese of the Hobart and related ICT security systems.

2.2 No computing or network device other than Archdiocesan issued equipment is to be physically connected to the Archdiocese network via a cable or any other physical connection device.

2.2.1 It is not permissible to physically connect any computing or network device to an Archdiocesan network outlet at any of the connected sites, unless it is issued by ICT Services.

2.2.2 Connection of non-Archdiocesan issued equipment is a security risk to the Archdiocese and may result in disciplinary action against the User or person allowing a guest to physically connect their device to an outlet.

2.3 An AOHTAS Guest Wireless Network is available for computing devices that require Internet access not issued by ICT Services. This network is typically used for external Presenters, Guest Speakers or Board Members.

2.3.1 The above is only means by which guest's devices can access Internet resources using the Archdiocese infrastructure.

2.3.2 Guest devices are not to be physically connected to any physical network outlet or join any other AOHTAS Wireless network within the premises of any site that is part of the Archdioceses' network. This is a security risk to the Archdiocese and may result in disciplinary action against the staff member organising the guest access.

2.3.3 The AOHTAS Guest Wireless network is not to be used for smart phone connectivity.

2.3.4 Guests will require a username and password to connect to the internet. A temporary username and password will be allocated on a "**Per-User"** basis. Guest accounts will be deleted after they are no longer required.

2.3.5 It is the responsibility of the staff member organising the guest speaker event or board meeting to advise ICT Services of the dates, duration and number of guest accounts required at the time of booking the event.

2.4 Electronic material created, or produced during the course of work or for work purposes by Users belongs to the Archdiocese under the intellectual property agreement signed by the staff member at commencement of employment.

2.5 Any intellectual property created by a volunteer using Archdiocese electronic equipment is to be regarded as part of that volunteer's contribution to the Archdiocese.

2.6 Staff are to ensure that all work created or produced as part of their work, processes or requirements is saved to the AOHTAS network share or system advised for their functional area, programme or Business unit.

2.7 Business Unit Managers are to ascertain the storage requirements of their programs and work with the ICT Manager in providing an appropriate storage solution for their programmes.

2.8 Business Unit Managers are to advice the ICT Manager in writing and in advance should their data requirements change or the business storage size needs to be increased. Storage requirements increases may be a result of programme changes or digitisation of paper records.

2.8.1 Any major changes to data storage is to be discussed with the ICT Manager and a formalised project plan implemented for any approved change.

2.9 Only work related data and information is to be stored on Archdiocesan shared resources. No personal data such as non-Archdiocese related work, personal images, movies and multimedia is to be saved onto any Archdiocese server share, system or resource.

2.9.1 Work data is not to be saved to personal cloud storage. Staff are to use the approved Archdiocese of Hobart solution.

2.9.2 Whilst data can be saved onto external hard drives, electronic media or a workstation hard drive, it is not to be the sole or primary location for data. It is a temporary holding for short term use i.e. for a PowerPoint presentation.

2.9.3 An exception to clause 2.9.2 may be applicable where there are no other feasible storage locations and after discussions have been had with the ICT Manager, to ensure adequate backup and security measures are implemented to meet any compliance requirements.

2.10 Any data saved to non AOHTAS approved network or system locations will not be supported or recovered by Archdiocesan ICT Services should the data become corrupted.

2.11 No client or confidential work information is to be stored on unencrypted USB devices or personal cloud storage accounts. This is a breach of privacy and compliance and may result in disciplinary or legal action.

2.12 It is the responsibility of all Users to ensure external USB or storage devices connected to their workstations are scanned for virus or malware prior to use.

2.13 Work related data on mobile devices and other portable devices such as USB storage is to be kept secure at all times.

2.14 Third Party Cloud services required for work purposes are not to be created with individual user account details. A generic AOHTAS account is to be created for the purpose of the Cloud access.

2.15 Business Unit Managers and Programme Supervisors are to advise ICT Services of their requirements prior to creating such an account.

2.16 The Archdiocese of Hobart approved cloud storage facility is to be used by staff.

2.16.1 Where an alternative cloud storage facility is required for business use, approval is to be sought from the ICT Manager prior to use.

2.17 Where a cloud storage facility is established, all account details including username and password are to be retained by the Business Unit Manager.

2.18 Business Unit Mangers and Programme Coordinators are responsible for following security protocols when there is a change of staff. This includes:

2.18.1 Changing password and permissions for access to third party cloud storage and services.

2.19 Work information or data is not to be shared externally to the Archdiocese unless it is in regards to work being carried out on behalf of the Archdiocese specifically agreed to by an immediate supervisor.

2.20 Only ICT Services staff are authorised to install software or firmware onto Archdiocesan equipment. No User is allowed to download, install or transfer programs or software onto Archdiocesan computer equipment or electronic media without the approval of the ICT Manager.

2.20.1 An exception to clause 2.20 is the installation of apps and updates for work issued smart phones. Whilst there are no restrictions on staff downloading apps onto smart phones they are to err on the side of caution. Apps often request access to contacts and location when being installed. Staff are to refuse all requests to access contacts and to ensure that no apps downloaded are able to access client details and information. Allowing access to work contacts by third party apps is a breach of work confidentiality agreement

2.21 New software requests or business solutions to be installed, purchased or tested for review are to be emailed to the ICT Manager for review and discussion with the Business Unit Manager or Programme Supervisor prior to any approval being given. Some Software approval requests

2.22 Access to existing approved software is to be requested through the ICT Ticketing system by the unit supervisor. Requests are to include reasoning and need related to work processes.

3. Email and electronic communication

3.1 Archdiocesan provided emails or electronic communication is the only approved media to be used for any work related communications.

3.2 Email or electronic communication is provided for staff and volunteers where it is required for their work activity by the Archdiocese.

3.3 Users are provided Internet and email access for work requirements. Private use is to be kept to a minimal level.

3.4 Users of the system are to be aware that personal (non-work related) use of these electronic facilities is a privilege and not a right. This privilege may be withdrawn at any time.

3.5 Emails and any electronic communications including websites, intranet, and all types of social media channels are a formal means of communication, i.e. they constitute a legal document. Emails and any electronic communications or digital assets can be subject to court orders for production as evidence in the course of litigation.

3.6 Archdiocesan provided emails are filtered for malware, security risk etc. prior to entering the AOH internal network. Whilst this system is robust and is the first tier of defence to protect staff it does not provide 100% complete protection from all risks and does not replace user awareness and responsibility of risks inherent with using electronic communications.

3.7 User awareness of appropriate and secure usage of email and electronic communication is a requirement prior to use of any such application.

3.8 Staff members have a personal responsibility to understand and be aware of the security risks inherent in email and other electronic communication usage and are to use these facilities with care.

3.9 Email is not a secure medium and can be intercepted through the internet. Sensitive or confidential information can be intercepted by a third party. There is no guarantee that communications sent through email will remain private.

3.10 There is no guarantee that emails sent will not be misdirected, forged, corrupted or delayed in transit. These issues are beyond the control of the Archdiocese's ICT infrastructure and the Archdiocese cannot be held responsible for corruption or loss of emails or other communications sent.

3.11 Staff and volunteers are to use emails and electronic communication in an appropriate manner, and are cautioned to avoid transmission of confidential information through emails.

3.12 The use of electronic communication should reflect the standard of professional conduct and ethics that would otherwise be maintained as an employee of the Archdiocese. Since email messages and electronic communication transmitted reflect on the Archdiocese, it is essential that staff retain a professional demeanour in all internal and external correspondence.

3.13 Whilst staff are issued with Archdiocesan provided emails for work purposes, this can be used for some personal correspondence; provided, it does not impede on work time and does not contravene the Archdiocese Workplace Behaviour Policy and Government Regulations.

3.14 Personal email account access and usage is not encouraged during work times.

3.15 There is a specific prohibition against inappropriate email or electronic communications use. This includes any content which is derogatory, sexually offensive or that may be prohibited on the grounds of discrimination set out in the *Sex Discrimination Act 1984* (Cwlth), the Tasmanian *Anti-Discrimination Act 1998*, the *Human Rights and Equal Opportunity Commission Act 1986* (Cwlth), and *Racial Discrimination Act 1975* (Cwlth) and the *Disability Discrimination Act 1992* (Cwlth) (e.g. sex, age, race & ethical belief) and any discriminatory comments on those grounds.

3.16 The content of any email or electronic communication must not bring the Archdiocese, its employees, members or associates into disrepute.

3.17 Inappropriate emails or electronic communication are not to be circulated or forwarded. Inappropriate is deemed as any item that can cause offense or disruption, either through humour, discrimination or bullying or is considered spam or that contravenes any Government legislation or the Archdiocese Workplace Behaviour Policy.

3.18 Care should be taken to ensure messages are addressed to specific recipients and should not be broadcast across the network indiscriminately

3.19 No information concerning the Archdiocese, its employees, volunteers, clients or associates may be sent to any other party without proper authority.

3.20 All emails sent using an Archdiocese email address for any work related correspondence is to have an indemnity disclaimer at the footer of the email.

3.21 It is the responsibility of Users of Archdiocesan emails to ensure that an indemnity disclaimer is visible at the bottom of any work related email correspondence sent including emails sent from Archdiocesan web mail.

3.22 An indemnity disclaimer is available as an email template on the staff intranet.

3.23 Standardised email signature templates specific to CatholicCare Tasmania are to be used by all CatholicCare employees when using work related email correspondence.

3.24 Various standardised email signature Templates specific to different CatholicCare Agencies and programmes are available on the staff intranet.

3.25 Staff personal signatures are not to be scanned nor copied as an image onto any digital asset including electronic documents.

3.26 An exception to the above rule, will only apply if the document is secured to disallow any copy or modifications prior to sharing the document/digital asset. The original document used is to be deleted and the secured unmodifiable document is to be kept as the original.

3.26.1 Images of staff signatures used on unsecured documents are a security risk and can be used for identity theft or fraud.

3.26.2 Alternate electronic signature products are legally binding and should be considered for e-transactional contracts. Australia's Electronic Transactions Act (1999) defines a regulatory framework for electronic transactions and states. "Documents signed online with legally compliant e-signature software are as valid and binding as traditional pen-and-paper documents."

3.27 Attachments to emails are limited to 15MB in total size including the email.

3.28 Large file transfers for sharing with external clients or suppliers are to use Archdiocese provided Cloud storage provisions. Assistance with large file transfers can be requested from ICT Services or Communications & Marketing Unit.

3.29 Users are to exercise caution and verify the legitimacy of an attachment received within email or any electronic communication prior to opening such attachment. Attachments opened are to be work related and not part of any scam, hoax, public communication chain etc.

3.30 Users are to verify authenticity of any links received within their email or electronic communication channel prior to click on the link. This includes links from non-work contacts, birthday greeting cards, phishing communications etc.

3.31 Users are encouraged not to enter any personal details, username or passwords onto any site that is unknown to them and has not been approved by ICT Services.

3.32 Personal responsibility is to be practised when using any electronic media or communication. Ignorance is not an excuse. Users are responsible for the consequences for web sites they visit or links they access within electronic communications.

3.33 Phishing or Malware sites accessed by clicking on links that have not been verified that result in Identity theft or fraud are not the responsibility of the Archdiocese or any of its Agencies.

3.34 All Users including volunteers are to be aware of the inherent risks associated with Internet usage when using Archdiocesan equipment.

3.35 User accessing Internet resources outside of the Archdiocesan WAN network are not protected by the Archdiocesan Firewalls. This includes all users with mobile devices when not working at any of the major WAN sites.

3.35.1 Mobile device users are to be vigilant when accessing web sites as they are not protected behind the Archdiocese firewall. Users not aware of the dangers should ask for clarification when reading this document from ithelp@aohtas.org.au or visit the following government site for further information http://www.cybersmart.gov.au/

4. Email Retention/Quota

4.1 All issued email accounts have a storage quota assigned to them. Once an email account has reached its storage quota, the account will be prevented from sending emails until the mailbox storage size has been reduced.

4.2 Quota sizes are issued based on work requirements and compliance needs.

4.3 Employees/Staff are responsible for housekeeping and for keeping their emails within the Quota assigned to them.

4.3.1 Employees/Staff and volunteers with email access are to manage their email storage sizes and to periodically clean out their mailboxes by deleting unnecessary and out-of-date emails and attachments.

4.4 Programme Managers are to approach ICT Services to organise appropriate training for their section should any staff or volunteer be unclear on how to manage their Archdiocesan provided mailbox.

4.5 Online Email archiving is provided by the Archdiocese of Hobart based on work requirements and compliance needs.

4.6 Only approved email archives will be protected by Archdiocesan backup processes.

4.7 Other forms of email archives will not be protected or supported by ICT Services

4.8 Business Units/Agencies required to retain emails for audit or government compliance are to advise ICT Services so appropriate retention and archival arrangements may be implemented.

4.9 The Archdiocese may need to keep documents which relate to and are considered important for audit or compliance purposes. These requirements are to be advised to the ICT Services for implementation of suitable email retention plan for the Business Units or Programme.

4.9.1 Documents requiring manual retention are to be printed and put into the relevant files.

5. Electronic Communication Ownership and Privacy

5.1 All email or electronic communications, created, modified or transmitted by, received from or stored on Archdiocesan storage or using Archdiocesan electronic systems are the property of the Archdiocese.

5.2 The ICT Manager and or ICT Services may access any email both incoming or outgoing or review backup facilities for the purpose of ensuring that this policy and guidelines are being adhered to or for any other purpose that the Business Manager considers relevant.

5.3 The Archdiocese reserves the right to restrict, delete, return or ban any message from being received and/or sent for any reason.

5.4 All Users must comply with the principles of the *Privacy Act 1988* (Cwlth) and the *Personal Information Protection Act 2004* (State) and relevant updates of these Acts

5.5 Any User who receives or views a message not intended for them is required to keep the contents confidential.

6. Internet

6.1 The Archdiocese provides Internet access to Employees/Staff and volunteers for work purposes.

6.2 No staff member is authorised to create an Internet site, blog, social media space etc. or Web presence for the Archdiocese or any of its Agencies without the written approval by both the Archbishop of Hobart and the Archdiocesan Business Manager

6.3 It is the responsibility of the Business Unit or Agency Head to ensure any public internet based site meets Internet compliance standards for security, standardisation and accessibility.

6.4 It is the responsibility of the Business Unit or Agency Head to ensure content promoted on Internet sites is monitored and updated to remain current and that it complies with legislation and the Archdiocesan Workplace Behaviour Policy.

6.5 Social networking or internet sites are to be created under the Agency name not an individual User's identity. Business Unit and Agency Heads are to follow the Archdiocese of Hobart Social Media Policy in regards to site creation including passwords, changes and access.

6.6 There is a specific prohibition against inappropriate internet use. This includes use to access or publish information which is derogatory, sexually offensive or that may be prohibited on the grounds of discrimination set out in the *Sex Discrimination Act 1984* (Cwlth), the Tasmanian *Anti-Discrimination Act1998*, the *Human Rights and Equal Opportunity Commission Act 1986* (Cwlth), the *Racial Discrimination Act 1975* (Cwlth) and the *Disability Discrimination Act 1992* (Cwlth).

6.7 Archdiocesan networked Internet access is filtered and usage is monitored. Requests for access to content types or sites that are blocked by default must be made in writing to ICT Services by the Business Unit Manager or Agency Head with the business reason for the access required.

6.8 Users are not to download software, shareware, freeware, media files or executable files from the Internet onto Archdiocesan network servers or connected workstations.

6.9 Users are to obey copyright, licensing or permission requirements in regards to any form of media or documents sourced from the Internet.

6.10 Any use of the Internet must not bring the Archdiocese, its employees, members or associates into disrepute.

6.11 Any personal (non-work-related) use of the Internet is a privilege and not a right. This privilege may be withdrawn at any time. This includes excessive use of streaming media or inappropriate usage of the Internet.

6.12 Inappropriate use of the Internet may result in disciplinary action.

6.13 Users are to gain approval by the Business Unit Manager or Agency Head and the ICT Manager prior to allowing the streaming of music, audio or video for work purposes. Such activities if not part of work requirements disrupt other users' access to the Internet.

Glossary

Name	Description
Archdiocesan network	This refers to the Archdiocesan of Hobart computing network infrastructure domain. This network authenticates users, computers and services to access Archdiocesan computing resources, services, applications, storage and data. · Members of this network are required to authenticate their identity to access resources based on their level of security and permissions. · This network also includes the physical sites that are part of the AOHTAS Private IP network.
Archdiocesan Wide Area Network	This refers to the Archdiocese of Hobart sites that are physical connected to the Archdiocesan network or joining different sites across the state to the same computing network physical infrastructure.
Cloud	Various services and resources accessed through the internet. These can range from application software, email, data storage, web sites and infrastructure services that are hosted off site. There are two main types of Cloud ownership Public and Private 1. Public Cloud – Services are subscription based. a. Services and storage is hosted outside of the organisation ownership and domain; many external users/organisations share the resources. 2. Private cloud – A secured private network where different sites are connected across the internet and services are provided for organisation members only a. The AOHTAS Private IP Network is a secured private cloud connecting Archdiocese and CatholicCare major sites together. b. Services and storage provided to users is managed and owned by the organisation.
Complex passwords	Password with minimum of 10 characters using alphanumeric combination, upper and lower case characters and symbols. Example: Th8b1Gd)g@ (thebigdogs)
Computing device	Any device that can store, manipulate, interact or view/access digital/analogue information in any form.
Data	Data is any information stored in any electronic format on any electronic or magnetic storage device. This includes structured and unstructured data. · Structured data is any record entered into databases and includes client, payroll, HR, ICT and financial records. · Unstructured data includes but is not limited to any publications, brochures, code, text, reports, plans, calculations, mathematical formulas, image, movie, video, voice recording, or any other information. Data and information are interchangeable within this document.
Direct Access	Only available on "Windows 8.1" and above portable workstations. Describes secured access to internal resources when outside the Archdiocesan network. A stable internet is required to connect using Direct Access. Once connected to the AOHTAS network resource access is the same as working onsite.
Electronic Material/Digital information / Digital Assets	Any data or information in any electronic/magnetic form or within a digital application. Examples include: documents, spreadsheet, video, images, audio or any electronic production used for electronic media.

Electronic media	Media that use electronics or electromagnetic or electromechanical energy for the end user (audience) to access content. This includes but is not limited to USBs, flash drives, memory cards, external/internal hard drives, DVD/CD, floppy disks, tapes, any visual or audio media, cameras, mobile/smart phones, or any recording devices.
Hybrid	Mix of on premise, private and public cloud services. Cloud services are linked to the business internal systems so services can communicate. Management is controlled by the organisation working within the public cloud parameters.
Malware	Malicious software that can infect an electronic storage device resulting in corruption of data both on the device and throughout the network, disruption of services, theft of identity or other malicious outcomes.
Mobile devices	Includes any portable electronic or magnetic form of computing and communications device. Current examples include laptops, tablets, smart phones, digital pens and other portable devices that store, manipulate, interact or is used to view/access data or information.
On premise	ICT Services and infrastructure is owned and physically located at the site local to users. External access to the Public internet is not required to access information.
Phishing	A disguised web site or email that looks legitimate however is a ruse for the receiver or web site visitor to divulge personal information especially in regards to passwords or other security information.
Social Collaboration	Ability to share and interact with other members irrespective of location. This includes the ability to share and manipulate any digital asset including messaging, video, voice, and or data manipulation on shared documents and sites.
Social Media Channels	Internet communication sites that allow collaboration between members. Sites can be based on similar interests, features of the site or ways of promoting or connecting to a wider world audience. Social Media Channels use digital assets as the main form of communication between members. Social Media Channels can include, web sites, intranet, forums, Instagram, Facebook, twitter etc. to name a few. A user login is required and some personal details to identify users and connect members. Blogs, likes, messaging, images, videos, document sharing and following other members etc. are features of social media and social collaboration.
Users	Any person that has permission to use ICT services provided for Archdiocesan network system
VoIP	Voice over Internet Protocol. This is basically voice being transferred over the internet. Telephone calls are made using the internet instead of dedicated analogue lines. VoIP calls can be made from a computing device or a mobile device. Phone Handsets used for VoIP would be considered a mobile device.
Workstation	A work computing device used by an employee for their normal work needs. Includes, stationery or portable computing devices, monitors and peripherals including printers, scanners etc.

ACCEPTANCE OF POLICY GUIDELINES

I *(Print name)*:…… of

Agency:……

confirm I have read and understand this Computing and Communications Usage Policy Agreement and agree to abide by the guidelines as stated in the policy. I have received a copy of this document.

Signed:…….. *Date…….*

Please return a signed copy of this page to HR & Compliance. This copy will be retained on your personal file.