ICT Acceptable Use Procedure

Section 1 - Purpose

(1) The Catholic Diocese of Maitland-Newcastle (the Diocese) seeks to provide its authorised users with secure and timely access to Information Communication Technology (ICT) Services to facilitate learning, teaching, administration, and other functions of the Diocese.

(2) The purpose of this procedure is to expand on the related Information Security Management System Policy (the policy).

(3) This procedure is intended to:

a. Provide a clear statement of responsibilities for all Authorised Users of the Diocese's ICT Services, including what constitutes acceptable and unacceptable use; and
b. Express the commitment of the Diocese in maintaining secure, effective, and reliable ICT Services.

Section 2 - Scope

(4) This procedure applies to all workers of the Diocese including its agencies.

(5) This procedure applies to other users including students, parents, carers and all users of the Diocese's ICT Resources and where not already covered, to ICT facilities, services and materials owned or managed by the Diocese, including Bring Your Own Device (BYOD).

(6) This procedure also applies to suppliers and service providers where the contract to provide services to the Diocese expressly refers to the application of this procedure.

(7) This procedure sets out the controls for:

a. Usage.
b. Privacy Expectations and Intellectual Property.
c. Acceptable use of email.
d. Unacceptable use of email.
e. Acceptable use of the internet.
f. Unacceptable use of the internet.
g. Use of Social Media.
h. Usage of Artificial Intelligence (AI).
i. Use of ICT Resources.
j. Use of Mobile ICT resources.
k. Additional responsibilities particular to mobile and portable devices.
l. Sharing of Images.
m. Consequences of inappropriate behaviour.

Section 3 - Responsibilities

ROLE	RESPONSIBILITIES
All staff, parents, students, third parties, volunteers and any other user of ICT resources	Fully understand the implications of ICT Acceptable Use Procedure.
Directors, Heads of Agencies, Heads of Shared Services	♦ Set the tone at Diocesan and agency level, by demonstrating commitment to and compliance with this procedure. ♦ Promote awareness of this procedure and implications for breaching this procedure; and ♦ Take disciplinary action where breaches are identified.
Head of Technology Services	♦ Approve the ICT Acceptable Use Procedure. ♦ Communicate and implement this procedure across the Diocese. ♦ Promote awareness of this procedure and implications for breaching this procedure; and ♦ Take disciplinary action where breaches are identified.
Technology Services	Monitor the use of the network and report breaches to the Directors or Heads of Agency where appropriate.
People and Culture	Ensure all workers and users are aware of and acknowledge the ICT Acceptable Use Procedure when access is granted to the Diocese's network and then every 12 months
Managers	♦ Ensure all workers are aware of and agree to the ICT Acceptable Use Procedure when access is granted to the Diocese's network. ♦ Promote awareness of this procedure and implications for breaching this procedure; take disciplinary action where breaches are identified.
Technology Services FSA/FSO	♦ Ensure that the authorised use of Diocesan ICT Asset or resources is consistent with principles, regulations and laws relating to the privacy and safety of school students, workers and Catholic Schools staff. ♦ Discuss with Principals their school's needs in relation to social media before official pages are activated. ♦ Be actively involved in the investigation and resolution of any reported incidents. ♦ Contact the Police and Office of Safeguarding in the suspected case of a worker accessing child pornography. The Criminal Code Act 1995 Volume 2 Subdivision D lists possession of child pornography as an offence. ♦ In the event there is a breach, ensure that the reporter of the breach submits an incident report in the Diocesan incident management system, MN Response. ♦ Take disciplinary action where procedure breaches are identified.

Section 4 - Procedure

Usage

(8) The Diocese provides computers and internet access to support the mission of the Church, facilitate learning and the administration of the agencies, and to enhance the opportunities for Diocesan students, staff and others who access our services.

(9) All ICT equipment remains the property of the Diocese or its agencies.

(10) Users are to utilise Diocesan computers, networks, and internet services for work or school-related purposes including BYOD in schools.

(11) Incidental personal use of Diocesan computers is permitted, if such use does not interfere with the individual's job duties and performance, with system operations or with other system users.

(12) Users must ensure that personally identifiable information remains confidential in communications concerning

individuals and staff.

Privacy Expectations and Intellectual Property

(13) Users' browsing activities, email, and instant message content, call records, and other systems metadata can be scrutinised. Such scrutiny will occur as the Diocese considers necessary as a reasonable management action and will be carried out in a reasonable manner.

(14) System administrators can access user data and log network and communication use, as part of their role.

(15) In reviewing and monitoring user accounts and information, the Diocesan systems administrators will respect the privacy of individuals. These people must not divulge or disclose such information to others unless required by a director or Head of Diocesan Agency, the Head of People and Culture, or State or Commonwealth Law (Australian Privacy Principles, 2001).

(16) If a system administrator discovers information that demonstrates a breach of this procedure during their duties, information about this breach will be reported to the Head of Technology Services, who will be responsible for liaising with the respective Director or Head of Agency or Head of People and Culture.

(17) If a breach has been committed directly by the Head of Agency the matter will be referred directly to the CEO (or delegate).

(18) System administrators within the Diocese include the Bishop, Head of Technology Services and delegated personnel as specified by the Bishop or the Head of Technology Services.

(19) Electronic communications and materials produced, sent, and kept by users remain the property of the Diocese and relevant Diocesan agency.

Electronic Mail

(20) The sender of an email has no control over the future distribution of the message. The following are technical realities of the use of emails:

(21) Email should be regarded as insecure unless it has been encrypted by the user before sending.

(22) Emails are hard to destroy. Even deleted emails are backed up and recoverable.

(23) Most software used to operate networks, including web servers, mail servers and gateways, log transactions and communications. These logs will normally include the email addresses of senders and recipients, and the time of transmission. System administrators can read the contents of emails sent and received by Diocesan networks (OAIC).

(24) The Diocese reserves the right to block any email messages suspected to contain any malicious or other inappropriate content.

Acceptable use of email in the workplace is defined as:

(25) Communication to others on work or school related matters connected with the goals and purposes of each respective agency.

Unacceptable use of email in the workplace is where email is used to:

(26) Distribute unsolicited email messages, including "junk email" or "spam" or other advertising materials, except in the case of agencies sending material of an advertising or promotional nature to users within the Diocese's system.

(27) Use Diocesan email distribution lists without authority or for the sharing of non-work or school related matters.

(28) Harass or discriminate against other users.

(29) Send abusive email.

(30) Defame other users, The Diocese, or another individual or organisation.

(31) Disclose personal information or contact details about another student, worker or user.

(32) Receive, maintain, or transmit pornography.

(33) Read another person's email or other protected files unless otherwise authorised by this procedure.

(34) Send or forward chain emails that may be interpreted as harassment by others.

(35) Send or forward to others jokes which may amount to sexual harassment or discrimination via email on an intranet or the Internet.

(36) Send anonymous messages which contain no details of the sender's name and affiliation.

(37) Unauthorised use, or forging, of email header information.

(38) Access non-Diocesan based email systems or accounts e.g. Hotmail, Gmail, or other email services. These externally provided systems cannot be guaranteed to have provided acceptable protection against viruses and other malware.

(39) Waste resources, time or the capacity of the system or the equipment. This is especially inappropriate for personal use or where productivity is directly affected.

(40) Without authority, destroy, alter, dismantle, disfigure, prevent rightful access to or otherwise interfere with the integrity of computer-based information and/or information resources including, but not limited to, uploading, or creating computer viruses.

(41) Use a third party's copyright material.

(42) Send sexually explicit, suggestive, or other harassing material.

(43) Distribute information that could reasonably be regarding as misleading or represents a conflict of interest with the Diocese.

Internet Access and Web Browsing

(44) Logs are maintained that record information on the sites which people visit. Keeping these logs is necessary for the routine maintenance, security and management of networks and systems. Information is logged automatically.

(45) Most content made available on websites (includes text, images, software, sound, and video clips) is protected copyright material. Accordingly, when browsing the Internet, copyright laws must be respected. However, under the Copyright Act 1968, the making of a temporary reproduction of a work while browsing the Internet is not an infringement.

(46) It may not be possible to tell if a web page is relevant until it has been read. The operation of web search engines can result in surprising and irrelevant results. Links on websites may also be misleading (OAIC). If you inadvertently open an inappropriate website, you should close the website immediately and keep details of the circumstances under which you accessed the site.

(47) All users have a dual responsibility to protect those in their care, e.g., clients, school students, or elderly

residents, from offensive material and to ensure that no one may be liable for transmitting offensive material.

(48) The Diocese reserves the right to restrict access to any Internet site suspected to contain malware or other inappropriate content.

Acceptable use of the internet in the workplace is defined as:

(49) Accessing information and resources for work or school-related matters connected with the goals and purposes of each Agency.

Unacceptable use of the internet in the workplace is where the internet is used to:

(50) Download sexually graphic material.

(51) Access websites that contain pornographic material.

(52) Participate in 'Chat Groups' or use other chat/instant messaging technologies for discussions unrelated to work or school.

(53) Subscribe to electronic mailing lists unrelated to work or school.

(54) Violate any Local, State, Commonwealth, or International Law.

(55) Conduct any non-Diocesan business activity for financial gain or commercial purposes.

(56) Download unnecessary information or unauthorised software.

(57) Violate Diocesan or third-party copyright or licensing agreements or other contracts.

(58) Seek to gain unauthorised access to any resources within or outside the Diocese.

(59) Waste resources, time or the capacity of the system or the equipment. This is especially inappropriate for personal use or where productivity is directly affected.

(60) Access sexually explicit, suggestive, or other harassing material.

Use of Social Media

(61) Use of social media, whether in a personal capacity or as part of a role within the Diocese, must be carried out in line with the Diocese's Media Policies and Procedures as referenced in the related documents section at the start of this document.

Acceptable Use:

(62) Social media should be used to support the mission of the Diocese, facilitate communication, and promote positive engagement within the community.

(63) Employees, volunteers, and representatives of the Diocese are encouraged to share content that reflects the values and mission of the Diocese, such as educational resources, community events, and inspirational messages.

(64) When using social media in a professional capacity, users should ensure that their posts are respectful, constructive, and inclusive.

(65) Personal use of social media should not interfere with work responsibilities or the performance of job duties.

Unacceptable Use:

(66) Users must not use social media to harass, bully, or intimidate others. This includes sending threatening or inappropriate messages, sharing offensive content, or engaging in any form of cyberbullying.

(67) It is prohibited to post or share any material that is fraudulent, harassing, threatening, bullying, embarrassing, sexually explicit, profane, obscene, racist, sexist, intimidating, defamatory, or otherwise inappropriate or unlawful.

(68) Users must not use social media to disclose confidential or proprietary information about the Diocese, its employees, or its clients without proper authorisation.

(69) Engaging in any activity that could harm the reputation of the Diocese or its members is strictly forbidden. This includes making negative or defamatory comments about the Diocese, its employees, or its clients.

(70) Users must not use Diocesan resources to access or post on social media for personal gain or to promote personal business interests.

(71) Students must not use email or any other means to bypass social media blocks put in place by the Diocese. Any attempt to circumvent these restrictions is considered a violation of this policy.

Use of ICT Resources

(72) The following guidelines exist on the general use of Diocesan computer and network facilities, in general:

(73) Users must not make contact through any form of information technology, with Children, young or vulnerable adult who are known through a user's role in the Diocese, for any relationship or contact outside a user's professional role unless such contact has prior approval from a manager.

(74) Users must not contact children, young or vulnerable persons, via any form of information technology, for the purpose of initiating or maintaining an inappropriate relationship.

(75) Users must not circumvent security controls, such as but not limited to using proxy servers to bypass internet filtering.

(76) Extensive use of Diocesan ICT Services for personal and private business is prohibited.

(77) Network accounts are to be used only by the authorised owner of the account for the authorised purpose.

(78) Users shall not disclose their account details or passwords to any other person.

(79) Users will maintain passwords that would not be easy for someone to guess and will change their password regularly in accordance with the Password Security Procedure.

(80) Users will log off or lock their workstations when unattended to prevent unauthorised use of their computer and credentials.

(81) Users shall not intentionally seek information on, obtain copies of, modify files, other data, or passwords belonging to other users, or misrepresent other users when using Diocesan ICT Services.

(82) All communication and information accessible via the network should be assumed to be private property.

(83) No use of the network shall serve to disrupt the use of the network by others.

(84) Malicious use of the network to develop programs that harass other users, infiltrate a computer or computer system and/or damage the hardware and software components of a computer or computing system, is prohibited. This

includes the introduction of malicious programs into the network or server including but not limited to viruses, worms, Trojan horses, Ransomware, and email bombs.

(85) The installation of unlicensed software for use on Diocesan computers is prohibited.

(86) The Diocese reserves the right to monitor the use of any Information Technology or Communications resource. Monitoring will be conducted in accordance with the NSW Workplace Surveillance Act, 2005. Users should be aware that acceptance of this procedure constitutes official notice that surveillance may be conducted under the Act.

(87) Diocesan ICT Resources must not be used to conduct illegal activities as defined by any local, state, or international legislation.

(88) Diocesan ICT resources must not be used to access any material which would be considered offensive or derogatory based on race, sex, or religion; or material which a reasonable person would deem unacceptable.

(89) Users must not attempt to gain unauthorised access to any system, network, or data. This includes attempting to bypass security measures or accessing resources for which they do not have explicit permission.

(90) Users must not engage in any activity that could harm or disrupt the ICT resources of the Diocese. This includes, but is not limited to, introducing malware, engaging in hacking activities, or using ICT resources for illegal or unethical purposes.

(91) Users must not use Diocesan ICT resources to harass, bully, or intimidate others. This includes sending threatening or inappropriate messages, sharing offensive content, or engaging in any form of cyberbullying.

(92) Users must report any suspected security breaches or misuse of ICT resources to the appropriate authority immediately.

(93) Users must adhere to all relevant laws, regulations, and Diocesan policies when using ICT resources.

(94) If users gain access to any system, network, or data that they are not authorised to access, they must report this to Technology Services immediately.

(95) Users must not access, read, forward, download, modify, or in any way use any information or resources that they are not authorised to access. Any such unauthorised access must be reported to Technology Services immediately.

Use of Mobile ICT Resources

(96) The Diocese provides mobile ICT equipment and resources to users with roles requiring them to be contactable when working away from their normal base, who regularly travel between sites or are on-call after hours.

(97) Users must be efficient, economical, and ethical in their use and management of these resources which are provided for organisational purposes.

(98) All users are responsible for ensuring the proper use and security of these resources in line with the rest of this procedure.

Additional responsibilities particular to mobile and portable devices include:

(99) Physical Security: Mobile ICT equipment must be always secured to prevent damage or theft.

(100) Safe Operation: Mobile ICT equipment must not be used while controlling a vehicle or other machinery. This is prohibited even if the road rules permit some hands-free usage as it has been shown that having a mobile phone conversation, regardless of using hands-free technology, while driving can increase the risk of a crash resulting in hospitalisation by four times (BMJ, 2005).

(101) Return of Equipment: All mobile ICT equipment must be returned to the Diocese or its Agencies on cessation of a user’s engagement.

(102) Security Lock Code: Users must ensure that their mobile devices are protected with a security lock code to prevent unauthorised access.

(103) Device Integrity: Users must not modify, jailbreak, or root their mobile devices. Any such actions can compromise the security and integrity of the device and the Diocese's network.

(104) Any loss, theft, or security breach involving mobile ICT equipment must be reported to Technology Services immediately so that the device can be remotely wiped.

(105) Personal Use: Diocesan-issued devices are not for personal use. Personal user accounts, apps, and services should not be used on Diocesan assets. Users may use their own personally owned devices for personal activities, but they must never use their personal devices for anything related to the Diocese.

Acceptable Use of AI

(106) The Diocese permits the use of specific generative AI tools and those that are part of the Dioceses approved software using Diocesan accounts. The use of any other AI tools, generative or otherwise is strictly prohibited unless authorised by Technology Services.

Acceptable Use:

(107) AI tools should be used to support the mission of the Diocese, facilitate learning, and enhance the administration of the agencies.

(108) Users are encouraged to utilise AI tools for educational purposes, content creation, and improving operational efficiency.

(109) When using AI tools, users must ensure that their activities are ethical, respectful, and in line with the values and mission of the Diocese.

Unacceptable Use:

(110) Users must not use AI tools to harass, bully, or intimidate others. This includes generating or sharing threatening, inappropriate, or offensive content.

(111) It is prohibited to use AI tools to create or disseminate misleading, false, or harmful information.

(112) Users must not use AI tools to access, read, forward, download, modify, or in any way use information or resources that they are not authorised to access.

(113) Any unauthorised use of AI tools must be reported to Technology Services immediately.

(114) Students must not use AI tools to cheat or complete work on their behalf unless specifically instructed to do so by their teacher or school.

Authorisation and Compliance:

(115) Users must seek authorisation from Technology Services before using any generative AI tools not explicitly permitted by the Diocese.

(116) All use of AI tools must comply with relevant laws, regulations, and Diocesan policies.

(117) Users must ensure that any data input into AI tools is de-identified and does not contain personally identifiable information unless explicitly authorised.

Reporting and Accountability:

(118) Any misuse or suspected misuse of AI tools must be reported to Technology Services immediately.

(119) Users are responsible for ensuring that their use of AI tools does not compromise the security, integrity, or reputation of the Diocese.

(120) All prompts and responses from AI tools may be logged and reported by system administrators to ensure compliance and security.

Acceptable usage of VPN services

Authorised VPN Services

(121) Only VPN services provided and approved by the Diocese are permitted for use.

(122) The use of any other VPN services is strictly prohibited.

Installation of VPN Software

(123) No VPN software, other than those approved by the Diocese, shall be installed on any diocesan assets. This includes, but is not limited to, laptops, desktops, phones, tablets, and servers.

Security and Compliance

(124) The use of unauthorised VPN services may result in the automatic locking of user accounts and revocation of access. This is due to our security systems detecting logins from geographically disparate locations, which is a key indicator of a security breach.

Enforcement

(125) Any violation of this policy will be subject to disciplinary action, up to and including termination of employment.

Sharing of Images

(126) Sharing of student, worker or customer images is to be for Diocesan purposes only.

Section 5 - Consequences of inappropriate behaviour

(127) A user's conduct and behaviour in relation to the use of email, internet, web browsing or use of ICT Resources may be deemed inappropriate if the contents of this procedure are found to have been breached.

(128) If so, a thorough and transparent investigation of the alleged breaches will take place. This investigation will be carried out by the director or Head of Agency and/or their delegate.

(129) Failure to comply with this procedure governing computer use may result in disciplinary action, up to and including dismissal.

(130) Offenders may be disciplined via the relevant Agency disciplinary procedures, which may include termination of their employment.

(131) Illegal use of Diocesan computers will also result in referral to law enforcement agencies.

(132) The possession, control, production, supply, or obtainment of child pornography for personal use, or use by another person, is an offence under Section 474.20 of the Schedule to the Criminal Code Act 1995.

(133) If a user is found to be accessing child pornography sites or possessing child pornography, the matter will be reported to the police, Office of Safeguarding and the Office of the Children's Guardian.

Section 6 - Document Review

(134) This procedure will be reviewed when there is a legislative change, organisational change, delegations change, technology change or at least once per year to ensure it continues to be current and effective.

Status and Details

Status	Current
Effective Date	9th December 2024
Review Date	9th December 2027
Approval Authority	Head of Technology Services (Chief Information Officer)
Approval Date	9th December 2024
Expiry Date	To Be Advised
Unit Head	Damian Wicks Head of Technology Services (Chief Information Officer)
Enquiries Contact	Mark Carbonaro IT Architecture and Security Manager Technology Services

Glossary Terms and Definitions

"Children" - Refers to people under the age of 18 years. [1] [1] Under the Children and Young Persons (Care and Protection) Act 1998, there is a differentiation between children (0-15 yrs) and young people (16-17 yrs). However, the Crimes Act 1900 and the Child Protection (Working with Children) Act 2012 define children as any person less than 18 years of age. The Children's Guardian Act 2019, other than for purposes of Part 6 Child Employment, also defines children as persons under 18 years of age. The National Catholic Safeguarding Standards defines children as "individuals under 18 years of age". The definition recognises that there is a graduation towards independence that begins for children prior to their 18th birthday, through adolescence increasing independence and self-determination is afforded a child, e.g. making some medical decisions independent of their parents etc.

"Vulnerable adult" - On 7 May 2019 Vos Estis Lux Mundi established a definition of vulnerability. The revised decree (27 March 2023) establishes that a vulnerable adult: means any person in a state of infirmity, physical or mental deficiency, or deprivation of personal liberty which in fact, even occasionally, limits his or her capacity to understand or will or otherwise resist the offence." Vos Estis Lux Mundi also states that "a person habitually suffering from the imperfect use of reason shall be equated with a minor". The National Catholic Safeguarding Standards (Ed. 2) apply the term 'adult at risk' which "means any person aged 18 years and over who is at increased risk of experiencing abuse". The term is very broad and significantly beyond what canon law deems to be vulnerable. The Diocese is guided by the understanding of vulnerability set out in Vos Estis Lux Mundi. To assist practical interpretation, the Diocese considers vulnerable adults as those who: ♦ have physical disability of sufficient severity as to make them dependent on another for assistance in everyday activities and self-care; ♦ have a chronic or persistent mental illness that significantly impedes their competence to self-determine their lives; ♦ have a developmental delay or other cognitive disability to a moderate or profound degree; ♦ is neurodiverse to a degree that ongoing functioning in society requires assistance and support from another; or ♦ becomes physically or mentally frail as a result of advanced years or personal history (e.g. having been in institutional or statutory care). Whilst a person may have a medical diagnosis or a statutory or other classification which evidences that person's vulnerability; it is not a prerequisite. For the purposes of this policy, the assessment of the diocesan worker that a person meets one or more of the criteria, based on credible evidence, is sufficient to determine that a person should be afforded the protections of being a vulnerable adult. Individuals and families (including children) or other relationship groups who are classified as refugees or asylum seekers by the Australian Government are also considered vulnerable. An asylum seeker is a person who has fled their own country and applied for protection as a refugee.

"Worker" - A person who carries out work in any capacity for an employer or 'Person Conducting a Business Undertaking'. This includes: ♦ employees; ♦ teachers; ♦ educators; ♦ contractors; ♦ apprentices;

♦ clergy; ♦ religious; ♦ student placements; ♦ trainees; and ♦ volunteers/unpaid . In the Catholic Diocese of Maitland-Newcastle, 'worker' includes those who carry out work in diocesan parishes, within diocesan agencies and as a part of the diocesan curia.

"User" - A user or authorised user is a person who has been provided with a username and password by the Diocese to access Diocesan ICT services. This includes workers, parents/carers and students.

"Bring Your Own Device" - (BYOD) Any digital device owned, leased, or operated by an authorised user of the Diocese when connected to Diocesan ICT Services.

"ICT" - Means information and communications technology within the remit of the Diocese or its agencies.

"ICT Asset" - Means any hardware, software, cloud-based services, communication devices, data centres or networks that are owned by the Diocese or provided by the Diocese, to users.

"ICT Resource" - Means any ICT service, ICT asset or digital information.

"ICT Services" - Facilities and services provided to an authorised user, including software, communication devices and computing infrastructure under the control of the Diocese (or a third party provided on the Diocese's behalf) that provides access to information in online or electronic format.

"Incidental personal use" - Means use by an individual user for occasional personal communications. Users are reminded that such personal use must comply with this procedure and all other related policies, procedures and rules.

"Mobile device" - Any portable, wireless computing device that can connect to the internet. This includes, but is not limited to, smartphones, tablets, wearables (like smartwatches), e-readers, portable gaming consoles, and other portable devices with internet connectivity.