



MINARAH
RABBI ZIDNI ILMA

ICT Policy

February 2024

Purpose

This policy is intended to protect the integrity of the Minarah network, to mitigate the risks and losses associated with security threats to computing resources and to ensure secure and reliable network access and performance for the Minarah community. This policy is necessary to provide a reliable campus network to conduct the College business and prevent unauthorized access to data. In addition, the College has a legal responsibility to secure its computers and networks from misuse.

Date of last review:	February 2024	Author:	Principal/s
Date of next review:	February 2025	Owner:	Principal/s
Type of policy:	State-wide (DoE) Tailored by school	Approval:	School Board
Key contract email:	principal@minarah.nsw.edu.au	Key Contact Number:	02 8783 9188

Positioning Within Minarah Operational Model

Component	Element
<input type="checkbox"/> Strategic Leadership and Planning	
<input checked="" type="checkbox"/> Monitoring, Reporting and Data	
<input type="checkbox"/> Governance and Accountabilities	
<input type="checkbox"/> Teaching and Learning	
<input type="checkbox"/> Culture, Ethos and Wellbeing	
<input type="checkbox"/> Curriculum and Assessment	
<input type="checkbox"/> Pathways and Enrichment	
<input type="checkbox"/> Parents and Community	
<input type="checkbox"/> Finance, IT & Estates	
<input type="checkbox"/> Our People	

Contents

Purpose	2
Policy Statement	4
Scope	4
1.0 Use of Minarah ICT Facilities	4
2.0 Network and Cyber Security Policy	6
3.0 Home and Shared Drives	7
4.0 Device (Computer/Laptop/Surface/iPad and other IT equipment) agreement Policy	7
5.0 Cyber Safety Policy	8
6.0 E-Mail Policy.....	9
7.0 Online and E-learning policy	10

Policy Statement

- Minarah ICT department is solely responsible for managing any and all Internet domain names related to the college (e.g. gvic.nsw.edu.au). Individuals, academic colleges/departments or administrative departments may not create nor support additional Internet domains without prior approval from ICT department.
- To ensure the stability of network communications, Minarah ICT department will solely provision and manage both the public and private IP address spaces in use by the College.

Scope

This policy applies to all Minarah faculty, staff, students, vendors/contractors, guest account holders, and any other agents who may connect to Minarah network computing resources. This policy also applies to all devices which are used by those individuals for network access, whether personally owned, College issued or otherwise obtained. These devices include but are not limited to workstations, laptops, tablets, smartphones, servers, consoles, controllers, and any other computing device which can communicate on Minarah networks.

1.0 Use of Minarah ICT Facilities

- Use of Minarah ICT facilities must be for the purpose of teaching, coursework, associated administration or other authorized use. No 'private/commercial' work is permitted without prior authorization from the college Principal/s.
- Minarah ICT facilities include the network, the virtual private network (VPN), computers, printers and the associated services e.g. software, data, email, Web, digital boards.
- A unique username and password are assigned to each User. Password details must be kept secret and account details must not be shared.
- Not disclose to others his/her Minarah login credentials or access or attempt to access ICT facilities at Minarah or elsewhere for which permission has not been granted or facilitate such unauthorized access by others.
- Monitor all activity on their account(s) and take the necessary and appropriate steps to protect their privacy.
- Always logout and secure their device after they are done working.
- Students are required to always follow their teacher's directions when using the college's e-learning devices (such as computers, laptops, iPads and others).
- Students are required to care for and always respect the college's e-learning resources.
- Students may not change any settings on college e-learning devices (including desktop background, browser themes, gadgets, widgets, mouse cursors and desktop icons) and will report any misuse to their classroom teacher or e-learning Leader.
- Students are required to immediately report anything that they see online that makes them feel uncomfortable or unsafe.
- Students are required to immediately report any misuse of college e-learning resources by another student, including inappropriate online behavior.
- Not display, store, receive or transmit images or text which could be considered offensive e.g. material of a sexual, pornographic, pedophilic, sexist, racist, libelous, threatening, defamatory, of a terrorist

nature or likely to bring the Minarah into disrepute.

- Not forge email signatures and/or headers, initiate and/or forward 'chain' or 'junk' or 'harassing' email.
- Not play unauthorized games. Respect the copyright of all material and software made available by the Minarah and third parties. and not use, download, copy, store or supply copyright materials including software and retrieve data other than with the permission of the Copyright holder or under the terms of the license held by the Minarah.
- Students/Staff are responsibilities to use computers/devices in a responsible, safe and ethical manner.
- Use all technology resources in an appropriate manner so as to not damage them.
- Student activities strictly prohibited include (but are not limited to:
 - a. Illegal installation or sharing of copyrighted materials.
 - b. Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic obscene, or sexually explicit materials.
 - c. Use of chat rooms for non-educational purposes.
 - d. Internet/Computer Games deemed inappropriate by teachers.
 - e. Downloading apps without teacher permission.
 - f. Spamming-Sending mass or inappropriate emails.
 - g. Accessing other students' accounts, files, and/or data.
 - h. Use of the college's internet for illegal activities.
 - i. Use of anonymous and/or false communications.
 - j. Sharing personal information online unless under teacher instruction to do so.
 - k. Transmission or accessing materials that are obscene, offensive, threatening, or otherwise intended to harass or demean.
 - l. Students will be expected to use the Network and Internet in a purposeful and responsible manner.
 - m. Students are encouraged to report any incidents of cyberbullying or inappropriate use of technology that they become aware of.
- Whilst the Minarah takes appropriate security measures against unauthorized access to, alteration, disclosure, destruction, or accidental loss of personal and other data it cannot and does not give any warranties or undertakings to the USER about security, confidentiality, or integrity of data, personal or other.
- The same applies to other ICT material submitted to or processed on facilities provided or managed by the Minarah or otherwise deposited at or left on its premises.
- Minarah will not be liable for any loss, damage, or inconvenience arising directly or indirectly from the use of, or prevention of use of, any ICT facility provided and/or managed by Minarah.
- Breach of these conditions may lead to College disciplinary procedures being invoked, with penalties that could include suspension from the use of all College computing facilities for extended periods and/or fines. Serious cases may lead to expulsion or dismissal from the College and may involve civil or criminal action being taken against the User.

2.0 Network and Cyber Security Policy

- All PCs, laptops, and other computing equipment are banned from connection to the Minarah data network. Unless such equipment was purchased through Minarah for the purpose of connecting to the College data network OR prior approval for connectivity has been granted by ICT.
- Under NO circumstances is a College PC or other computing equipment to be unplugged from a network jack. This policy excludes College portable equipment.
- Unauthorized PCs, laptops, and other computing equipment that are connected to the college's network are in violation of the Minarah ICT Policy.
- Unauthorized access to the Minarah equipment/cabling rooms is also prohibited. • Unauthorized access to Minarah networking equipment (firewalls, routers, switches, etc.) is prohibited. This includes port scanning or connection attempts using applications such as SSH/SNMP, or otherwise attempting to interact with Minarah network equipment.
- Internet access is restricted and managed by ICT department. This means that staff and students at Minarah have restricted access to the Internet and will only be able to access approved websites that are deemed educationally relevant and safe.
- Restricted sites are therefore blocked and any attempt to access these sites is recorded and the user is identified.
- When students are using the Internet at home, which includes the use of programs and applications that are used at college, that the college's Internet filtering and website management is not applicable. It is important to ensure that home internet is protected and filtered and access to such resources is closely monitored.
- The use of local firewall technology should be considered to protect sensitive data. Any firewall installation must be done in consultation with the ICT Department and meet their requirements.
- All network addresses, including IP addresses, will be allocated and administered by the ICT Department.
- Physical connections to the College backbone may be made only by the ICT Department. No extensions or modifications to the physical infrastructure of the ICT network, including wireless, may be made without first obtaining permission from the ICT Department. This includes the addition of network switches, hubs, wireless access points router devices, and cabling other than patch cable to a provided network wall socket. Any network infrastructure equipment or wiring is managed and controlled by the ICT Department.
- The ICT Department may, on behalf of the Minarah, and subject to appropriate consultations or approval from the College Principal/s, restrict excessive use of the backbone bandwidth.
- Some activities deemed inappropriate include, but are not limited to:
 - a. Attaching unauthorized network devices, including but not limited to wireless routers, gateways DHCP or DNS servers; or a computer set up to act like such a device.
 - b. Engaging in network packet sniffing or snooping.
 - c. Setting up a system to appear like another authorized system on the network (trojan).
 - d. Other unauthorized or prohibited use under this or any other Minarah policy.
 - e. ICT Department will maintain and monitor traffic logs for all networks, devices, and systems for security auditing purposes.

- In the event of unacceptable network events occurring on a LAN, ICT has the right to gain access to and inspect the configuration of devices or equipment on that network and to request the immediate removal of any devices or equipment that it believes could be the source of the problem.
- In the event of unacceptable events on a LAN causing problems on another part of the College network or on an external network, ICT Department has the right to disable any part of the LAN, as necessary, in order to remove the source of the problem. While every effort will be made to contact the system custodian, Head of Department and/or other appropriate persons, this may not always be possible. All services will be reconnected at the first opportunity.
- Failure to comply with the rules for connection to the College network may result in immediate disconnection from the network.

3.0 Home and Shared Drives

- All users have an allocated home drive.
- All Departments have their own Shared Drive.
- All user data is fully backed up every night.
- Data is recovered upon request to the ICT Department. Normal turnaround for a restore request is one business day.
- Please note that neither your personal home drive nor any shared drives should be used to store personal pictures (.jpeg, .png, bmp, tiff), audio (.avi), or music files.
- These personal files greatly increase the costs of our backups and slow down the daily and weekend backup process.
- To preserve space on the network and to ensure the backup process continues to remain seamless, please delete any non-curriculum-related files.

4.0 Device (Computer/Laptop/Surface/iPad and other IT equipment) agreement Policy

- The device (Desktop Computers/laptops/iPads/Surface and others) will always remain the property of Minarah College. On cessation of employment with the College, for whatever reason, the device must be returned to the College.
- The device will only be used for the purpose of College-related work. It will not be loaned to or used by a third party for any purpose.
- The device will not be used to access or store any material that can be classified as illegal or obscene.
- No Staff/Student/Board/League and Shurah to alter/replace software that is preloaded onto the machine. This might violate the licensing arrangements.
- The device will not be covered by the College's insurance policy in case of damage or loss due to theft or otherwise.
- It is understood that while reasonable wear and tear are justifiable, any cost incurred resulting from willful damage due to improper use, care, or otherwise will be user responsibility.

5.0 Cyber Safety Policy

- The College will maintain cyber safety practices at college which aim to maximize the benefits of technology to student learning and minimize risk.
- Responses to and any concerns regarding misuse or cyber-bullying occurring at college will be prompt and in accordance with Minarah Wellbeing policy.
- While supervision and usage out of college hours falls under parental authority, support will be provided to parents and students experiencing cyber-bullying occurring out of college hours with accordance to the Minarah Wellbeing policy.
- The College is responsible for Addressing cyber-bullying or misuse occurring at college.
- The College Provides relevant education for the students and the wider college community regarding Cyber Safety.
- Implementation of Policies which address staff and student well-being.
- Students are required to respect the rights and safety of others in their use of technology.
- Students are required to follow directions and procedures from staff regarding Cyber Safety.
- Conduct themselves in a manner reflecting the values of the College.
- Refrain from any misuse especially that which gives rise to allegations of bullying, harm to others or attacks on reputation.
- Refrain from uploading any content related to the College onto the internet including but not limited to: posting images of the College logo, teachers, uniforms or buildings.
- Refrain from Sending or receiving naked or sexually explicit content.
- Refrain from Defaming the reputation of another (including the college's own reputation).
- Refrain from Criminal offences including those related to and including pornography, stalking or assault.
- Refrain from any usage that would bring the college into disrepute.
- Parents are required to work in partnership with the college when the college is addressing misuse or Cyber- bullying which occurs at college.
- The breach of this policy will result in strict disciplines action according to the Minarah Wellbeing policy.

6.0 E-Mail Policy

- Staff and Students are provided with the email address who agrees to abide by college policies.
- All staff and teachers should assume that when sending and receiving information emails privacy cannot be guaranteed. Please take extra care to ensure that email is addressed to the correct recipient.
- If a complaint is raised that alleges improper use of the college email account, the ICT Staff with Principal/s's written approval will carry out an initial investigation. If the complaint appears to have a reasonable basis the matter will be referred to the College Principal/s so that further investigation will be considered in accordance with college policies and regulations.
- Staff and Students are provided with the college email account for the conduct of college related business.
- Personal email use is permitted if it doesn't disrupt the staff and students from the conduct of the college business.
- The inspection of the email account may only be undertaken upon seeking permission from the College Principal/s and the College Board of Directors in writing. It is not necessary to seek the former staff member's permission before such information can be inspected.
- Students will Report any e-mails containing inappropriate/abusive language and/or subject matter to their teacher or coordinator.
- College email accounts are to be used for college-based activities only.
- Students may not open/respond to any emails, attachments or links in an email from anyone they don't know or trust.
- Staff/Students are expected to regularly clear their email account.

7.0 Online and E-learning policy

Minarah will use e-learning to enhance teaching and learning opportunities for students. This allows experiences with a variety of applications related to NESAs Curriculum standards. Minarah recognizes the growing field of e-learning within society and the need for students to be active, safe and responsible users of digital technologies.

- Minarah online and e-learning policy in the guideline of cyber safety, cyber security and Minarah Wellbeing policy requires students to use the device and other online learning platforms in a safe and respectful manner.
- Students should not share the login credentials with others.
- Students should not post or upload the photos or other contents which are inappropriate.
- When using the e-learning platform for learning, students must always use language and behavior that is appropriate, respectful and safe.
- All replies and posts must relate to their learning and the learning of others.
- Students are required to dress in modest clothing while in the online e-learning teaching session.
- Students must identify a safe, comfortable, quiet space in the home where they can work effectively and successfully.
- Complete tasks with integrity and academic honesty, doing their best work.
- Submit work that is authentic and their “own” adhering to fair use of copyright material and plagiarism regulations.
- Do their best to meet timelines, commitments and due dates
- Students are required to communicate proactively with their teachers if they cannot meet deadlines or require additional support.
- Use live recording and recorded lessons for intended use.
- Students are not to record or upload lessons onto social media or share with others.

Document Control

Publication date:	February 2021	Review Date:	February 2024
Version number:	v1.3		
Applies to:	All Minarah Staff		
Responsible Review Officer:	Principal/s		
Approved by:	Minarah Board	Meeting Date:	

Revision History

Version	Revision Description	Revised By	Date
v1.0	Authorized	Jay Halai	February 2021
v1.1	Template Changes	Jay Halai	February 2022
v1.2	Review	Samina Ali	March 2023
v1.3	Review	Samina Ali	February 2024