INFORMATION COMMUNICATION AND TECHNOLOGY POLICY

PURPOSE

To ensure that the safety and integrity of MRAEL's and ATCNB's data, physical information technology infrastructure and software deployments are not impeded or negatively impacted in any way through the misuse of the company's Information Systems.

To ensure all users of the company's Information Systems are aware of their personal accountabilities and the resulting implications of the misuse of these Information Systems.

To provide transparency to the users of the company's Information Systems in relation to the level of monitoring, surveillance and auditing that occurs within the company's Wide Area Network.

To comply with:

- Standard 4.1 of the National Standards for Group Training Organisations

SCOPE

This policy applies to all users of MRAEL Limited's and Australian Trade College North Brisbane's (ATCNB) facilities, including all MRAEL Limited employees, ATCNB employees, students, apprentices, trainees, all contracted service providers with access to MRAEL or ATCNB facilities and other users.

Throughout this policy 'company' shall denote both MRAEL and ATCNB, unless otherwise stated.

POLICY

The intranet, Internet, electronic mail (email), mobile services, video conferencing and Instant Messaging (IM) are important business and educational tools that can enhance workflow and student learning, increase productivity and help users perform a variety of tasks; as such they should be used in an efficient, lawful and ethical manner.

ACCOUNTABILITIES

Intranet, Internet, email, mobile services, video conferencing and IM access is provided for officially approved purposes only. I.e. business purposes or student educational purposes.

Intranet, Internet, email, mobile services, video conferencing and IM usage should be able to withstand public scrutiny and/or disclosure. Unauthorised access, intentional misuse and transmittal or storage of material that might bring the company into disrepute is prohibited.

Users should not create, knowingly access, download, distribute, store or display any form of offensive, defamatory, discriminatory, harassing, malicious or pornographic material.

Electronic messages, electronic communication logs and electronic files are subject to surveillance, record keeping, archiving, freedom of information and legal process.

All users are required to comply with company policy and are bound by law to observe applicable statutory legislation relating to personal data, company data, public records, copyright and other forms of intellectual property and misuse of information and facilities.

The company will not be held responsible for the loss of any personal data that has been saved to its hard drives, mobile devices or networks.

USER RESPONSIBILITY

All users are expected to take reasonable precautions to protect intranet, Internet, email, mobile services/data, website information and IM systems against unauthorised access, illegal and inappropriate use, disclosure, modification, duplication and/or destruction.

Specifically this includes:

- Not allowing any other individual to use your network account.
- Not using other user's network accounts.
- Logging off computers and laptops that have been left logged on prior to using them.
- Understanding and complying with the security rules of these services.
- Not providing or allowing inappropriate access to information and not discussing it with others.
- Not providing third parties with unauthorised or unsupervised access to information.
- Being accountable for authorising or allowing access to information you create on behalf of the company (not applicable to students).
- Not attempting any unauthorised access to information and systems, whether internal or external, including email services and intranet and Internet services or company websites.
- Maintaining security, complexity and confidentiality of user ID's and passwords. Do not provide this information to any other party including ICT personnel.
- Not writing down passwords.
- Changing your password immediately if you suspect your account has been accessed by another user.
- Locking or logging off of unattended desktops and laptops.
- Locking screens using PIN, Password or Swipe Code on all mobile devices.
- Ensuring company electronic records of continuing value are not destroyed prior to their capture on the appropriate official company record-keeping system (not applicable to students).
- Reporting of any damage, to either hardware or software, to ICT personnel immediately.
- Reporting of any identified or supposed security vulnerabilities or breaches to ICT personnel.
- Following directions of supervisors (if worker) or teachers or trainers (if student) and other authorised personnel.
- Staff are required to maintain confidentiality with reference to student and family records and information, as outlined in privacy legislation. Where appropriate, the company will ensure the privacy of staff, student and family records through restricted access to records by relevant staff responsible for maintaining such information.

PERSONAL USE
(THIS SECTION DOES NOT APPLY TO STUDENTS)

Use of the company's communication systems, such as email, for personal use is permitted within reason. Company resources are not to be used for individual commercial activities.

ACCEPTABLE USE

Any information systems provided on a company network or any Information Technology equipment provided by the company can only be used for its intended purpose. I.e. business purposes or student educational purposes.

Business use includes any activity that is conducted for purposes of accomplishing official business, professional duties including research and, where appropriate, professional development. Student educational use includes any activity that is conducted for purposes of accomplishing educational outcomes, such as research, class work, preparation of assignments, study and assessments.

Users will be held personally accountable for any use of the company's ICT equipment, intranet, Internet, email, mobile services, video conferencing and IM services that does not comply with these principles.

INAPPROPRIATE USE

Users should not use intranet, Internet, email, mobile services, video conferencing or IM to:

- Execute unapproved applications and executables.
- Download software, unless they receive appropriate authorisation (for students, this would be instructions from a teacher, trainer or other authorised personnel) and comply with licensing requirements and established policies to check all such software for computer viruses.
- Run software directly from media such as USB.
- Attempt to access any secure area of the network you have not been granted explicit access to.
- Attempt to modify any aspect of the system via direct file access and/or Windows Registry editing.
- Attempt to access or modify log files or system logs.
- Be in possession of any form of "hacking" or "cracker" software, script, code or packet sniffing software regardless of how harmless it may appear.
- Use third party proxy systems or third party VPN software to bypass MRAEL or ATCNB content filtering systems.
- Attempt to guess passwords with brute force.
- Make copies or distribute copies of company software.
- Use ICT systems for duplication of copyright material.
- Save personal data such as digital music or photographs to company computers, laptops and network servers.
- Disrupt communication and information devices through such means as mass emailing or transmitting files which place an unnecessary burden on company resources.
- Access inappropriate Internet sites.
- Download, distribute, store or display offensive or pornographic graphics, images or statements or other material obtained from inappropriate Internet sites.
- Access non MRAEL or non ATCNB online chat services.
- Download, distribute, store or display material that could cause offence to others, for example offensive material based on gender, ethnicity or religious and political beliefs.
- Distribute defamatory, obscene, offensive, bullying or harassing messages.
- Distribute confidential information without authority.
- Distribute private information about other people.
- Register with websites or organisations that require an email address to complete registration unless specifically related to company business (if employee) or courses and curriculum (if student).

Users may not:

- Disrupt or interfere with the use of intranet, Internet, email, mobile services, video conferencing or IM services.
- Without authority destroy, alter, dismantle, disfigure, prevent rightful access to or otherwise interfere with the integrity of ICT equipment/hardware, intranet, Internet, email, mobile services, video conferencing or IM services.
- Misuse company resources, including human and computing resources.
- Reply to illegitimate email and "spam" using MRAEL or ATCNB Mail Servers.
- Make attempts to bypass security or filtering systems.

Students are expected to respect the privacy and ownership of others' work at all times. This includes not plagiarising information they find on the Internet and presenting it as their own work, or copying work of other students, with or without permission, which is held in students' electronic files.

RECORDINGS

'Recordings' in this section includes photos, voice recordings and video recordings, but excludes the video surveillance referred to in the Video Surveillance section of this Policy.

Electronic devices with recording capabilities must not be used in any place where a recording device would normally be considered inappropriate by a reasonable person. This includes in change rooms and toilets or any situation which may cause embarrassment or discomfort to others.

Recordings of person/s at company premises, or of person/s performing an activity or function directly associated with company operations (irrelevant of who owns the recording device), are not permitted unless:

- the person/s being recorded have been explicitly informed of the recording, prior to partaking in the recording; and
- no person/s being recorded overtly object to the recording; and
- the recording is lawful.

Any such recordings must not be published in a public forum (for example, posted to a website or to social media) without express permission being obtained from those recorded, prior to distribution.

If a worker of the company intends to record an ATCNB student, the worker must first obtain express permission from the College Manager or the Deputy Principal.

In addition, prior to recording, the company must obtain written consent from the person/s being recorded (or if the person/s being recorded are under 18 years of age, their parent/guardian), if:

- the recording is intended to be used by the company for the purpose of public relations, promotion, advertising, media or commercial activities; or
- the recording is intended to be posted online or published in any public forum.

DATA MANAGEMENT

(THIS SECTION DOES NOT APPLY TO STUDENTS)

The following points outline data management practices which must be adhered to when creating business related files, folders and data within the company's Wide Area Network or on any company Information System (e.g. Microsoft Outlook).

- Data quotas that are implemented must be adhered to and requests for lifting of or increase to quotas will not be agreed to. This includes but is not limited to network folder size, mailbox size, email attachment size limitation, My Documents folder size, Z:\ storage space.
- Network folders' default order must be alphabetical.
- Network folders must not include any of the following characteristics:
  - Folder paths which include more than 256 characters (system limitation)
  - Prefixed with special characters (e.g. ~ ' ` ! ?) in attempt to make them the first subfolder within a directory. This makes keyboard navigation of sub folders extremely difficult.
  - Numbered folders (e.g. 1. Charlie, 2. Alpha, 3. Beta) in attempt to change the order of subfolders within a directory. This makes keyboard navigation of sub folders extremely difficult.
  - Prefixed with letters (e.g. aaaaa_Folder2 or zzz_Folder1) in attempt to change the order of subfolders within a directory. This makes keyboard navigation of sub folders extremely difficult and locating of folders unintuitive.
  - Username related folders within company network drives (e.g. William's Folder).
  - Redundant looping folder structures (e.g. \Marketing\MRAEL\Apprentice Services\ Marketing\)

PRINTING

(THIS SECTION ONLY APPLIES TO ATCNB STUDENTS)

- Printer and photocopier usage is for work directly related to your learning only.
- Printing shall not be deliberately wasted or misused.
- Students are not to remove new blank paper from printers and copiers.
- Students are not to use any new blank paper from paper reams.
- Privately supplied paper is not to be used in printers and copiers.
- Overhead Transparency paper/plastic is not to be used in any printers or copiers without prior approval.
- Sticky label paper or similar “Avery Label” sheets are not to be used without prior approval.
- School Based (ASBA) students are required to pay for printing once their initial print credit of $2 runs out.
- Printing for ASBA students is currently charged at 9.5c per black and white A4 page, or 38c per colour A4 page. These rates are doubled accordingly for A3 or duplex printing.
- School-based Student Apprentices are required to ensure they have enough printing credit on their account before class.
- A print credit balance is capable of going negative, should you only have partial credit available when printing. This negative credit will need to be repaid before additional credit is available for further printing. Additional money can be added to your account by using the Vending Machine located at the A33 Photocopier Room window.
- Any trace of colour on a predominately black and white document that is printed to a colour machine will be charged at colour printing rates.
- Any documents left in paused print queues will still be charged once printing resumes.
- Documents that jam whilst printing will normally reprint automatically at no additional cost once the paper jam is cleared.

MONITORING AND INSPECTION

The company reserves the right to monitor any or all intranet, Internet and mobile related activity and to monitor and inspect any or all email messages and IM chat logs sent or received by users of company ICT resources, in order to:

- Identify inappropriate use.
- Identify cyber-bullying.
- Protect system security.
- Maintain system performance.
- Modify content filtering.
- Determine compliance with contracts, legislation and company policy.

These monitoring and inspection activities include but are not limited to the following:

- Access and examination of specific types of messages e.g. large messages or messages containing executable, audio visual files, movie files, command files and/or pictures, in order to identify inappropriate use or to maintain system performance.
- System security auditing.
- Access and examination of messages in specific circumstances, such as where an individual’s message volume is high or at the peak periods of the year or on a random sampling basis, in order to identify inappropriate use or to maintain system performance.
- Monitoring and inspection can apply to personal, business or educational use of intranet or Internet services and personal, business-related or education-related email messages.
- Account login history.
- File auditing.
- Internet browsing history.
- Print and photocopier usage.
- Hardware monitoring.
- Live viewing of individual computer monitors.
- Video surveillance (refer section below, Video Surveillance – ATCNB).

All external incoming calls to the main phone numbers (extensions 900 and 999) are recorded. External callers are greeted with an automatic message advising that their call is recorded. These calls are then transferred to other extensions and will then continue to be recorded.

VIDEO SURVEILLANCE
(THIS SECTION ONLY APPLIES TO ATCNB)

In order to protect the security of staff and students, ATCNB has installed video surveillance cameras at various locations around the College grounds. It is the policy of ATCNB to protect the privacy of staff and students who may be filmed by these cameras.

Surveillance cameras are placed in selected classrooms, workshops, internal foyers/hallways and exterior areas of the campus.

In locations where video cameras are located, clear signs are in place to alert any person on the College grounds that they may be videoed. The cameras are in operation 24 hours per day, seven days per week, in the locations indicated.

In order to protect your privacy ATCNB follows the procedures set out below:

1. Provided no incident has been reported in an area under video surveillance, all recordings are deleted within approximately 30 days without being viewed.
2. Recordings are stored in a secure location which can only be accessed by ICT personnel, the College Manager, Deputy Principal and the ATCNB Student Services Coordinator.
3. If an incident occurs in an area under surveillance, the recordings referring to that period of time will be viewed by ICT personnel, the College Manager, Deputy Principal and the ATCNB Student Services Coordinator only. If another staff member is required for identifying a student then they will view the recording under direct supervision of one of the staff listed above.
4. Should the recording provide information which has bearing on the incident, the police may be notified and the recordings will be made available to them.
5. Parents will be notified if a recording containing an image of their child has been passed on to police.

ATCNB is aware that from time to time students may be videoed near the time of an incident where they are clearly not guilty of any offence. ATCNB will do everything it can to protect the privacy of these students by destroying the recordings within 30 days or as soon as permission is received from the police.

CONSEQUENCES OF POLICY VIOLATIONS

Violations of this policy by workers may lead to disciplinary action (including dismissal) and/or action by the relevant regulatory authorities.

Violations of this policy by students may lead to:

- Disciplinary action.
- Reduced access and performance to Internet browsing for your account. (All work is still to be completed possibly in own time.)
- Removal of access to ICT resources. (All work is still to be completed possibly in own time.)
- Explanation of behaviour to parents and/or caregivers.
- Request for reimbursement of expenses resulting from malicious acts or purposeful damage.
- Suspension.
- Termination of enrolment.

COMPLIANCE

All individuals within the Scope of this policy are responsible for ensuring that this policy is adhered to.