The BUSY School Ltd

Acceptable Use of IT&T Services Policy

Purpose: The purpose of this policy is to manage the appropriate use of information technology and telecommunication services by students and employees at The BUSY School.

Scope: All Users of IT&T including students, parents and employees, including full-time, part-time, permanent, fixed-term and casual employees, as well as contractors, volunteers and people undertaking work experience or vocational placements.

Status:	Approved	**Supersedes:**	v.1 (Feb 2022)
Authorised by:	Board Chair	**Date of Authorisation:**	26/04/2023

References:

- The BUSY School (TBS) IT Equipment Loan Agreement
- TBS Discrimination, Harassment and Bullying Policy
- TBS Procedures for preventing and responding to incidents of bullying (including cyber bullying)
- TBS Student Code of Behaviour
- TBS Privacy Policy
- The BUSY Group Information Technology & Telecommunications Procedure
- The BUSY Group Cyber Security Incident and Data Breach Response Procedure
- TBG Information Security or Privacy Incident Reporting Form (online via Folio)

Review Date:	Bi-Annually	**Next Review Date:**	26/04/2025

Policy owner: The BUSY School Ltd - Board of Directors

Policy Statement

All Users at The BUSY School (TBS) have the right and responsibility to utilise information technology and telecommunications (IT&T) services as essential teaching, learning and business tools. TBS expect this technology to be utilised to its full capacity to provide the most valuable learning and teaching environment to the benefit of all. TBS also expects Users to demonstrate acceptable use via safe, lawful and ethical behaviour whenever using IT&T services.

This Policy applies to the management of all types of IT&T services, as defined in the 'Definitions' section below. This Policy applies on the school premises, when undertaking remote learning as well as during school activities such as excursions, camps, and extra-curricular activities, whenever TBS IT&T services are utilised, whether or not such use occurs on TBS premises.

TBS reserves the right to restrict User access to IT&T services if access and usage expectations are not met or are breached, however where possible restricted access will not disrupt the provision of the educational program within the school. Users should also note that breaches of this Policy may result in disciplinary action or legal proceedings.

This Policy also applies to personal electronic devices (including BYOD laptops, mobile phones, tablet devices, etc.) which are used to access any services provided by The BUSY Group (TBG)[1] directly or indirectly. Use of personally owned equipment which requires any form of connection to TBG resources must be approved by the CEO of TBS and TBG Information Technology Services (ITS) department.

[1] TBG provides corporate services to TBS which is outlined in a Service Level Agreement between the two entities. Corporate services include Information Technology and Support. Therefore, some IT&T services in this policy may be supported by services and roles provided by TBG.

Definitions

- IT&T – means information technology and telecommunication.
- IT&T services – includes but is not limited to IT&T networks, systems, facilities and devices, as defined below and includes those owned, leased, or otherwise used by the school.
- IT&T facilities and devices – includes but is not limited to computers (including desktops, laptops, netbooks, palm and handheld devices, PDAs, tablets, eBook readers, smart watches, VR devices and related devices such as monitors, keyboards and mice), telephones (including mobiles, iPhones and smart phones), removable media (such as USBs, DVDs, BlueRays and CDs), radios, or other high frequency communication devices (including microphones), television sets, digital or analogue players and records (including DVD, Blu-Ray and video), cameras, photocopiers, facsimile machines, printers (and other imaging equipment such as scanners), Smartboards, projectors and screens, teleconferencing devices.
- IT&T network and systems – electronic networks, internet, email, web mail, social media, fee-based web services, software, servers.
- Personal electronic devices – includes all types of mobile and smart phones, smart watches, laptops, tablets, cameras and video recorders, hand-held game devices, music devices, USBs, PDAs, eBook readers, other palm and handheld devices, and other equipment, as determined by the school, and owned by students.
- User - any person that accesses or uses TBGs IT&T equipment or infrastructure regardless of device, medium or location, including, but not limited to, its employees, students, parents, customers and participants.

Responsibilities

School Responsibilities

TBS acknowledges its responsibility to:

- develop and implement this Policy to ensure the full utilisation of IT&T services as essential teaching, learning and business tools within acceptable use parameters
- communicate this Policy to Users, including students, parents and employees
- keep appropriate records, monitor and report on any issues related to inappropriate IT&T services
- encourage Users to contribute to a healthy school culture

Employee Responsibilities

At TBS employees as Users have additional responsibilities to:

- uphold the school's Policy on this issue via their own safe, lawful and ethical use of IT&T services
- provide guidance and model appropriate behaviour for use of IT&T services in the classroom
- take reasonable steps to prevent and appropriately respond to any instances of inappropriate use by students and other Users of IT&T services,
- immediately raise any potential information security or privacy incidents via the internal incident report.

Student Responsibilities

At TBS students as Users have additional responsibilities to:

- uphold the school's Policy on this issue by ensuring the appropriate use of IT&T services via safe, lawful and ethical behaviour
- report any breaches of this Policy to the campus Principal

Usage Guidelines

All Users of TBS IT&T are expected to exercise responsibility, use the resources ethically, respect the rights and privacy of others and operate within the laws of the State and Commonwealth. This includes TBS policies and occupational health and safety obligations to employees and students.

Examples of acceptable use includes:

- Engagement in school activities, remote learning tasks and assignments set by teachers, including the conducting of general research, or accessing online references for school activities and projects
- Development of text, artwork, audio and visual material for educational purposes as directed and approved by school staff
- Communicating or collaborating with other students, teachers, parents/caregivers, or experts as a part of school activities

It is important to realise that when an IT&T network and systems is used inappropriately, there is potential for legal action both against the company and against the individual. In order to protect TBS, Users, unacceptable use of the IT&T network and systems is strictly prohibited and will result in disciplinary action by the campus Principal.

Examples of unacceptable use includes:

- Illegal purposes, or in support of such activities that may violate Local, State or Federal laws. This includes not adhering to copyright laws regarding use of content, software, information, and attributions of authorship
- Potentially or actually jeopardising the reputation of TBS through the access or distribution of inappropriate or illicit material, material that is in contravention of relevant State and Federal Legislations, or material that contravenes the values and philosophy of the TBS to internal or external individuals or organisations
- Using profane, obscene, offensive, racist, terrorist, sexist or inflammatory speech, or personally attacking any individual or entity
- Posting, accessing or transmitting material which is defamatory, vilifying or may amount to bullying and/or harassment
- Sending or posting information that is defamatory to TBS, its products/services, colleagues and/or customers
- "For profit" personal activity
- Stealing, using, or disclosing someone else's password without authorisation
- Damaging, vandalism or loss of IT&T equipment due to neglect
- Attempts to undermine, ‘hack’ into and/or bypass hardware and software security mechanisms in place
- Copying, disclosing, transferring, examining, renaming, or changing information or applications belonging to another User unless given expressed permission to do so by the individual responsible for the information or applications
- Violating the privacy of individuals by accessing accounts or reading email or private communications, unless individuals are specifically authorised and granted access for an explicit purpose
- Preventing the use or disrupting the performance of TBS or any other organisation's IT resources
- Transmitting and sharing data (including to personal email addresses) which is not authorised for distribution, including copyright infringements, trade secrets, personally identifiable data, or proprietary information, without proper authorisation and/or security
- Introducing malicious software onto the company network and/or jeopardising the security of the organisation's electronic communications systems
- Sending or posting chain mail, solicitations, or advertisements not related to business purposes or activities
- Passing off personal views as representing those of the organisation, or to misrepresent oneself or TBS
- Excessive distribution of jokes, gossip and rumours
- Where it conflicts with an employee’s conditions of employment

IT Environment

Applications

TBS utilises many software applications to facilitate day-to-day activities of the organisation. All applications available to individuals for use are shown on the Apps list within a User account profile. Users are not permitted to install any unauthorised applications onto IT devices. All requests for additional applications and access must be requested in writing through IT Support (ITS).

Devices

Users are provided with devices that suit the requirements of their position. All Users are responsible for ensuring that provided equipment is kept in a clean and tidy professional image, as well as ensuring that they are not damaged or misused. Any damage must be immediately reported to the campus Principal. Only TBS devices are allowed to access TBS and TBG IT&T networks and systems. Use of IT&T systems on personal devices is not permitted without prior written authorisation by ITS.

Email

The email system and email transmissions are the property of TBS and as such, TBS is responsible for the administration of the system. As they are considered official records of the organisation ownership of email messages rests with TBS, and as such authorised Employees have the right to access any material in an email account at any time. Monitoring of email accounts may occur at any time.

Internet

Use of the internet is permitted and encouraged, where such use supports the goals and objectives of the business. The internet must not be used in such a way as to significantly interfere with the purpose of such use or expose TBS to cost or risk of liability.

Passwords

The creation and safekeeping of passwords is a fundamental part of IT security.

- Users are not to save usernames and passwords which allow primary access to a number of other systems
- Users are not permitted to share their username and passwords for the system or any application
- Users are responsible for any actions made through their usernames and passwords

Passwords must:

- Have a minimum of 14 characters
- Include a capital letter
- Include numbers and or symbols
- Be changed at first log on from the generic password
- Be changed at regular intervals as requested by ITS

For Mobile Phone Passcodes you must:

- Have a minimum of 4-digit passcode
- Ensure settings are set to lock after 30 seconds or less of no activity

Students Personal Electronic Devices including Mobile Phones

Students are encouraged to avoid bringing valuable personal technology devices including mobile phones to school as there is a risk of damage or theft. If brought to school it is at Owner's own risk.

Students who choose to bring electronic devices/mobile phones to school must have them switched off and securely stored during teaching and learning sessions. Exceptions may be granted by the principal, or by a teacher.

Students must display courtesy, consideration and respect for others whenever they are using personal technology devices. Any student without exemption who is found using their phone/wearable devices during teaching and learning time will have the phone or device confiscated and returned at the end of the day. Repeated violations of this policy may result in suspensions and/or cancellations of enrolments.

Recording voice and images

Every member of the school community should feel confident about participating fully and frankly in all aspects of school life without concern that their personal privacy is being invaded by them being recorded without their knowledge or consent.

We uphold the value of trust and the right to privacy at TBS. Students using personal technology devices to record inappropriate behaviours or incidents (such as vandalism, fighting, bullying, staged fighting or pranks etc) for the purpose of dissemination among the student body or outside the school, by any means (including distribution by phone or internet posting) builds a culture of distrust and disharmony.

Students must not record images anywhere that recording would not reasonably be considered appropriate (e.g. in change rooms, toilets, or any other place where a reasonable person would expect to be afforded privacy).

Recording of events in class is not permitted unless express consent is provided by the class teacher.

A student at school who uses a personal technology device to record private conversations, ordinary school activities (apart from social functions like graduation ceremonies) or violent, illegal, or embarrassing matter capable of bringing the school into public disrepute is considered to be in breach of this policy.

Even where consent is obtained for such recording, the school will not tolerate images or sound captured by personal technology devices on the school premises or elsewhere being disseminated to others, if it is done for the purpose of causing embarrassment to individuals or the school, for the purpose of bullying[1] or harassment, including racial and sexual harassment, or where without such intent a reasonable person would conclude that such outcomes may have or will occur.

If students are involved in the following, they will be in breach of this policy:

- Recording; and/or
- Disseminating material (through text messaging, display, internet uploading etc); and/or
- Knowingly being a subject of a recording.

Breach of this policy may be subject to discipline (including suspension and recommendation for exclusion).

Students should note that the recording or dissemination of images that are considered indecent (such as nudity, or sexual acts involving children), is against the law and if detected by the school will result in a referral to the Queensland Police Service (QPS) and/or other relevant authority.

Text communication

The sending of text messages that contain obscene language and/or threats of violence may amount to bullying and or harassment or even stalking and will subject the sender to discipline and possible referral to QPS. Students receiving such text messages should ensure they keep the message as evidence and bring the matter to the attention of the school office.

Assumption of cheating

Personal technology devices may not be taken into or used by students at exams or during class assessment unless expressly permitted by staff. Staff will assume students in possession of such devices during exams or assessments are cheating. Disciplinary action will be taken against any student who is caught using a personal technology device to cheat during exams or assessments.

Recording private conversations and the Invasion of Privacy Act 1971

It is important that all members of the school community understand that under the Invasion of Privacy Act 1971, ‘a person is guilty of an offence against this Act if the person uses a listening device to overhear, record, monitor or listen to a private conversation’. It is also an offence under the Act for a person who has overheard, recorded, monitored or listened to a conversation to which s/he is not a party to publish or communicate the substance or meaning of the conversation to others.

Students need to understand that some conversations are private and therefore to overhear, record, monitor, or listen to such private conversations may be in breach of this Act, unless consent to the recording from all participants is appropriately obtained.

Special circumstances arrangement

Students who require the use of a personal technology device in circumstances that would contravene this policy (for example to assist with a medical condition, or other disability, or for a special project) should negotiate a special circumstances arrangement with the Campus Principal.

Reporting Security Incidents

IT security is a top priority when providing User access to TBS IT&T infrastructure, facilities or devices.

TBS staff are to immediately report to ITS should they believe that there has been a cyber-incident or data breach. Refer to the *Cyber Security Incident and Data Breach Response Plan* for further information. Staff that are found to be negligent, resulting in a data spill, may be held personally and/or financially responsible.

Compliance and Monitoring

Delivery of IT&T services are provided through TBG ITS Department within Corporate Services. TBG reserves the right to monitor all electronic communications and IT&T facilities and devices for the purposes of compliance, auditing, security or investigative purposes. The ITS team can be contacted at ITSupport@TheBUSYGroup.com.au

Version Control

Version no.	Date Effective	Approved by	Changes
1.0	February 2022	▪ Approved by TBS Board of Directors	▪ Initial draft version
2.0	April 2023	▪ Endorsed by TBS Governance, Compliance and Strategy Committee; ▪ Approved by TBS Board of Directors	▪ Aligned to ISQ template. ▪ Version control ▪ Review date bi-annually ▪ Consolidation of Mobile phone, use of personal technology and IT Equipment Loan Agreement

Appendix 1

The BUSY School Ltd

IT Equipment Loan Agreement

Purpose: From time to time, The BUSY Schools (TBS) may loan IT equipment to a student as a tool to assist remote learning. This agreement is to ensure that all users of borrowed TBS IT infrastructure are aware and accept responsibilities of the features, uses, and requirements of the equipment provided.

Scope: This agreement outlines the expected usage of IT equipment provided by TBS to students. IT equipment includes laptops, applications, user accounts, media, portals, email, internet access (including Wi-Fi/internet dongle), and any future technologies that TBS may issue students to aid learning.

Ownership

- TBS retains ownership of all IT equipment loaned to a student.
- Only software purchased or approved by TBS, and installed by TBS, can be used on TBS equipment. It is illegal to copy copyrighted software contrary to the Licence Agreement.
- All Internet data that is composed, transmitted and/or received by TBS systems is considered to belong to TBS and is recognised as part of its official data. This is therefore subject to disclosure for legal reasons or to other appropriate third parties.
- TBS reserves the right to monitor usage of all provided IT resources. All sites and downloads may be monitored and/or blocked if they are deemed to be harmful in any way.
- TBS does not guarantee against, nor shall it be responsible for, the destruction, corruption or disclosure of personal material on or by its IT resources.

Responsibilities

It is the responsibility of all students to utilise IT systems as they are intended and in a responsible manner. Students shall only access applications, files, data, and protected accounts that are their own, that are publicly available, or to which they have been granted authorised access.

Acceptable Use

Examples of acceptable use includes:

- Engagement in school activities, remote learning tasks and assignments set by teachers, including the conducting of general research or accessing online references for school activities and projects.
- Development of text, artwork, audio and visual material for educational purposes as directed and approved by school staff.
- Communicating or collaborating with other students, teachers, parents/caregivers or experts as a part of school activities.

Unacceptable Use

Abuse or deliberate misuse of IT equipment is strictly prohibited and will result in disciplinary action by the Campus Principal. Examples of unacceptable use includes:

- The viewing of pornographic, illicit material or deliberate attempts to use material that is illegal or which would be regarded by reasonable persons, as offensive.
- Posting, accessing or transmitting material which is defamatory, vilifying or may amount to bullying and/or harassment.
- Damage, vandalism or loss of IT equipment by neglect.
- Any ‘for profit’ use of IT equipment.
- Knowingly download viruses or other programs capable or breaching or damaging TBS network security.
- Attempts to undermine, ‘hack’ into and/or bypass hardware and software security mechanisms in place.
- Committing plagiarism or violating copyright laws.

- Sending chain letters or spam email.
- Violating the privacy of individuals by accessing accounts or reading/recording/distributing email or private communications unless individuals are specifically authorised and granted access for an explicit purpose.

Agreement

Any person that accepts access to TBS IT resources agrees they are aware of all requirements in relation to acceptable use of hardware and software and will follow all guidelines and instructions as outlined in this and any other relevant documentation.

- Students must ensure that they log on and off the systems correctly to ensure the continued serviceability and security of the system.
- Students are not permitted to install any applications without prior authorisation from the school.
- All passwords are to remain confidential with the allocated individual only.
- All devices are to be locked when not in use or unattended and stored in a safe and secure location.
- Students are not permitted to circumvent any user settings or guidelines, which may affect the security protocols required by the company.
- Students are to save all company documentation and information within allocated drives and online resources such as OneDrive. Information is not to be stored on local hard drives, desktops or any form of cloud storage repository such as Drobox, personal OneDrive accounts, Google Drive etc. Students must ensure that they do not use external hard drives or USBs without prior authorisation and registration through TBS.
- Students are required to report to the school immediately if:
    - a device is damaged, lost or stolen,
    - they receive or obtain data and/or information to which they are not entitled.
    - they become aware of breaches of security and/or confidentiality.
    - they become aware of any inappropriate use of TBS provided IT resources.
- Students are required to return all loaned IT equipment should they cease to be a student of TBS or if requested by the Campus Principal.
- All equipment should be returned to the school in the same condition as received, including any accessories and attachments. Students may be required to reimburse TBS for any costs incurred for IT equipment that is damaged, lost or stolen whilst in their possession. The Campus Principal will have sole discretion in deciding if costs are to be recovered from the student after consideration is given to the circumstances involved.

The following is to be read and completed by both the student and parent/legal guardian:

□ We have read and understood the IT Equipment Loan Agreement.

□ We agree to abide by the above rules.

□ We are aware that any breaches may result in disciplinary action, including my/my child’s immediate removal from access to the system for a specified period and in relation to the severity of the offence.

Student Name: ……………………………… ID: ……………………………… Year: ………………………………

Type of Device: ……………………………… IT Device Serial Number and ID: …………………………………..

Student Signature: ……………………………… Date: …/…/…

Parent/Guardian’s Name: ……………………………… Parent/Guardian’s Email / Phone: ………………………………

Student Signature: ……………………………… Date: …/…/…