ICT Acceptable Use Policy

AUP2020-1.2

Purpose:	The purpose of this policy is to manage the appropriate use of information, communication and technology services by students and employees at school		
Scope:	Students 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:** Computer Use Policy	
Authorised by:	CEO	**Approval Date:** 25th March 2019	
References:	Privacy Policy Anti-harassment Policy Anti-bullying Policy Positive Behaviour Policy Student Code of Conduct		
Reviewed:	2 Years	**Next Review:** 25th March 2021	
Responsibility:	Head of Campus	**Point of Contact:** Services Manager	

Policy

All students and employees at The Spot Academy have the right and responsibility to utilise ICT services as essential teaching, learning and business tools. The Spot Academy expects this technology to be utilised to its full capacity to provide the most valuable learning and teaching environment to the benefit of all. The Spot Academy also expects students and employees to demonstrate acceptable use via safe, lawful and ethical behaviour whenever using ICT services.

This Policy applies to the management of all types of ICT services, as defined in the "Definitions" section below. This Policy also applies on the school premises, as well as during school activities, such as excursions, camps and extra-curricular activities whenever The Spot Academy ICT services are utilised.

The Spot Academy reserves the right to restrict employee or student access to ICT services if access and usage requirements are not met or are breached. However, restricted access will not disrupt the provision of the educational program within the school. Employees and students should also note that breaches of this Policy may result in disciplinary action or criminal proceedings.

Definitions

- **ICT** – means information, communication and technology.
- **ICT services** – includes but is not limited to ICT networks, systems, facilities and devices, as defined below and includes those owned, leased or otherwise used by the school.
- **ICT facilities and devices** – includes but is not limited to computers (including desktops, laptops, netbooks, palm and handheld devices, PDAs, iPads, tablets, eBook readers and related devices such as monitors, keyboards and mice), telephones (including mobiles, iPhones and smart phones), removable media (such as USBs, DVDs, BluRays 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.

- **ICT 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, 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.

Responsibilities

The Spot Academy acknowledges its responsibility to:

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

ICT Support Requests

An ICT Support request can be logged via email to: **support@tsa.qld.edu.au**

Or via the following url: **https://thespotacademy.on.spiceworks.com/portal**

Please ensure when logging these requests that appropriate information is included; such as the device type, a description of the fault or request. Photos or screenshots are very helpful in identifying faults. Also, any relevant fault codes or what applications are being used when a fault occurs.

School staff must make requests for ICT Support through the support email or portal as a direct approach may indiscriminately be missed.

The support email or portal will ensure the job is logged and actioned appropriately so that appropriate change management occurs. This also allows communication to be recorded via email to assist with regular updates.

Students

Students are able to gain access to the school's Internet system by using desktop computers or school distributed iPad's whilst being supervised by staff. Students should be aware that when using school computers and Internet they are agreeing to the following:

- Only software purchased or approved by the school, and installed by the school, can be used on school equipment. It is illegal to copy copyrighted software contrary to the Licence Agreement. No software or data on the school computer system may be copied. Printing from CD-ROM or downloading and printing from the Internet is allowed for the purpose of school related study and research. Abuse or deliberate misuse of computer equipment will result in discipline by the Head of Campus and may include being banned from using all school electronic facilities for up to one term.

- Deliberate attempts to seek or use material that is illegal or which would be regarded by reasonable persons, as offensive is not permitted. The college administration has the final say in deciding what is or is not offensive in the college context, but will be guided by Section 85ZE of the Commonwealth Crimes Act which states that a person shall not knowingly or recklessly: 'Use telecommunication services supplied by a carrier in such a way as would be regarded by reasonable persons, as being in all circumstances, offensive.' **Use of the Internet in an offensive manner can result in criminal prosecution**.

- Students should be aware that all Internet access will be logged.

- If students are found misusing their access to the Internet or email by, for example, sending chain letters or abusive letters or accessing offensive material they will be referred for disciplinary action, and access to the network will be denied for a period specified by the Deputy Principal.

- The school is particularly concerned that school's computers & iPads are not used for bullying or harassing another student. Students found using the school's system or any non-college electronic device, including mobile phones, for cyber bullying should expect severe disciplinary action, up to and including expulsion.

- 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' computer files.

Staff

All staff members should be aware of the following in relation to their use of school technology:

- **Copyright -** Only software purchased or approved by the college, and installed by the school, can be used on school equipment. It is illegal to copy copyrighted software contrary to the Licence Agreement. Printing from CD-ROM or downloading and printing from the internet is allowed for the purpose of school related study and research. Software copying must be in accordance with legal requirements, and 'pirate' software is not permitted on any school owned computer.

- **Offensive material -** Deliberate attempts to seek, use or transmit material that is illegal or which would be regarded by reasonable persons as offensive is not permitted. Should offensive materials be received by staff members, they should be destroyed immediately. The school administration has the final say in deciding what is or is not offensive in the school context, but will be guided by Section 85ZE of the Commonwealth Crimes Act which states that a person shall not knowingly or recklessly: 'Use telecommunication services supplied by a carrier in such a way as would be regarded by reasonable persons, as being in all circumstances, offensive.' **Use of the Internet in an offensive manner can result in criminal prosecution**.

- ***Employer Liability*** - the college owns all messages and transmissions conducted through its system and therefore is legally responsible for all messages and transmissions. Staff should be aware that the school's computer system records all email and internet usage and, although *records of usage are not monitored on a systematic basis, nor are random checks undertaken on email and Internet usage by staff, should an issue arise in relation to email and Internet usage, the relevant records would be accessed.*

- **T*echnology Harassment*** – the college complies with all anti-discrimination legislation. Staff should be aware that email harassment and/or technology harassment can occur on any of the grounds of discrimination. The college will not tolerate email and/or Internet harassment. Any issue involving harassment or discrimination could result in disciplinary action.

- **Privacy** - Staff are required to maintain confidentiality with reference to student and family records and information, as outlined in privacy legislation. Where appropriate, the college will ensure the privacy of staff, student and family records through restricted access to records by relevant staff responsible for maintaining such information. Staff will be made aware through this policy and other appropriate forums e.g. staff meetings, of the need to maintain information security.

- **Access** - Computer systems at the school are protected by password access as well as physical barriers where possible. At no time should third parties be given unsupervised access to school records. Access to student, staff and family records will be given only on the authorisation of the CEO or his/her delegate where required by law or statutory authority. Staff should ensure that confidential documents or records are not left on desktops to be viewed by third parties, after-hours staff etc. Students are not to be given access to any sensitive account information under any circumstances. This includes administration passwords, staff computers, student information or wireless passwords to access the Internet. Staff must ensure that any information supplied to them relating to "access" is not displayed

in view of students or the public and is kept confidential.

- **ICT Equipment** – All ICT equipment supplied to staff are for the purpose of work-related activities. The Spot Academy retains all ownership of devices and content stored on them. Personal use is allowable provided it is not excessive and within the constraints of the ICT Acceptable Use Policy. Employment related data takes precedence over personal data. ICT resources may be accessed or monitored by Authorised Persons at any time without notice to the user. Authorised Persons must have a valid reason for accessing or monitoring use of The Spot Academy ICT resources. All supplied ICT equipment is to be handed in prior to or on the final day of employment. Failure to do so may result in final payment of wages being withheld or costs associated with replacement equipment being deducted. The Spot Academy retains the right to disable ICT equipment and related accounts in breach of this ICT Acceptable Use Policy. It is the responsibility of the staff member to remove personal data when relinquishing equipment at the end of employment. The Spot Academy takes no reasonability for the loss of personal data stored on work related devices.

- **Viruses** – the school attempts to prevent and/or detect viruses by ensuring suitable virus detection software is maintained on computer networks within the school. External disks will not normally be accepted into school computer systems. If an external disk is used on a school computer, it must be scanned for viruses prior to being used. No shareware type external games disks should be used in a school computer. Files downloaded from the Internet are to be scanned for viruses. If files are in a zipped format, they are to be scanned prior to and after extracting the zipped file. Emails with attached files are also to be scanned for viruses. Please contact the IT Coordinator if you detect a virus on school equipment.

- **Security –** Staff should report any security breach, including suspected security weaknesses and software malfunctions, to the college' system to the IT Coordinator immediately when they become aware of the breach. Staff members should be aware that staff involvement in a security breach is considered serious and may result in an official warning, counselling or termination of a staff member's employment according to the severity of the breach.

- **Emails – staff are asked to follow the procedures below when using the college's email system:**

- ***Use of disclaimer -*** All email messages should have the following Disclaimer included below your 'signature': *Disclaimer: Whilst every attempt has been made to ensure that material contained in this email is free from computer viruses or other defects, the attached files are provided, and may only be used, on the basis that the user assumes all responsibility for use of the material transmitted. This email is intended only for the use of the individual or entity names above and may contain information that is confidential and privileged. If you are not the intended recipient, please note that any dissemination, distribution or copying of this email is strictly prohibited. If you have received this email in error, please notify us immediately by return email or telephone (07) 5628 3300 and destroy the original message.*

- In the context of the school's Risk Management Strategy, *where appropriate*, email messages containing information or advice to parents/students/ college personnel and/or other organisations, should include the following Disclaimer (or similar): *The contents of this message are provided without responsibility in law for their accuracy or otherwise, and without assumption of a duty of care by the School.*

- ***Viruses*** - ***For incoming email*** – As *a matter of course all email attachments are checked automatically by virus protection software*. If there is any uncertainty about a file, the IT Coordinator should be consulted. Any files that end with .COM or .EXE should be first saved to hard disk and then scanned for viruses. If the source of the email is not known it should probably be erased.

- ***For outgoing email*** – It is unlikely that any .COM or .EXE files will need to be sent. If they do, the files must be virus scanned before sending.

- ***Use for official purposes*** - Email is recognised as an official form of correspondence and therefore care should be taken to ensure that spelling, grammar and format are appropriate to the professional standards required for school communications. Where appropriate, copies of email messages should

be filed accordingly for future reference and access.

- ***Use for personal purposes*** - The use of work email addresses for personal purposes is **not** permitted. This includes registering access to user accounts such as subscriptions, personal banking, e-commerce etc. This also allows more efficiency in navigating through work related email correspondence. Email facilities must not be used for any individual commercial activities.

- ***Absence from School*** - Individual staff members are responsible for the regular checking of their email messages. Staff should make arrangements for the checking of their email during any periods of leave. Alternatively, for staff on a period of extended leave, arrangements can be made to have email forwarded to another address within the school. The appropriate arrangements should be made through the IT Coordinator. Email 'out of office' alerts are to be activated when staff commence leave and should state an alternative contact and include a return to work date.

- ***Action on emails*** - All email messages should be actioned within appropriate timeframes. School emails are important for the day-to-day function and important communication within the school and must not be ignored. Messages that are intended for another member of staff can be simply forwarded to that staff member.

- ***File Management -*** Email will work more efficiently if not clogged up with unwanted emails. If certain emails need to be kept, it is worthwhile creating new folder(s) to keep these safe. It is important to delete messages, when no longer required, from three areas – Inbox, Sent Files and Deleted Files. Good practice would be to delete the files once a day if they are no longer required.
- ***Copyright -*** As with all documents, staff should ensure that copyright provisions are followed in relation to materials transmitted by email.