Section: Operations
Number: 2.26B
Version: 1
Page: Page 1 of 7
Approved: Executive Team
Date: May 2018
Review: May 2020

STUDENT IT POLICY

GUIDELINES FOR USE

PREAMBLE

This Policy applies in conjunction with to the existing School Policies of;

- Student Social Media Policy (2.43)
- Electronic Communications Policy (2.18)
- LTIP User Guide (1.13A)
- LTIP Policy Guide (1.13B)

The School accepts that the use of digital and online technology and environments can be an effective education and social tool and that such media is regularly used by the community.

The School's ICT network is provided for students to conduct research, study, and communicate with others.

Student use of the ICT Network must take place in accordance with the following guidelines and procedures.

The School believes that its students should behave in a manner that does not negatively affect or bring into disrepute the reputation of the School. The School also recognises that the misuse of digital and online technology and environments can cause both damage to the School's reputation and seriously affect the welfare of its students.

However, the School believes it is important for its students to have a clear understanding of its expectations of how digital and online technology and, in particular, Social Media should be used. This policy sets out these expectations.

Nothing in this policy is to be interpreted and/or applied in a manner that affects the applicability of other School policies, especially the School's Bullying policy, concerning student behaviour that may be applied in the event of student misuse of digital and online technology, including Social Media.

Similarly, nothing in this policy is to be interpreted in a manner that restricts the application of State and Commonwealth laws governing individual behaviour, which apply in the community outside the School. The School will fully support the application of these laws within the School.

The following practices using School local and wide area networks are prohibited:

- Use of the Network for political or commercial purposes;
- Electronic communications via the Network in a manner that is contrary to School policy;
- Use of the Network to disrupt the educational and administrative functioning of the School;
- Use of a School Network account of anyone but the authorised owner of the account;
- Use of the Network to allow reproduction of copyrighted material without written or explicit permission;
- Use of the Network to access, or attempt to access, material that is deemed inappropriate for School use.

PRIVACY

Student storage on Network servers is subject to the same privacy provisions as lockers, etc. It is the responsibility of students to ensure that their account password details remain private. The School may review communications logs, web-browsing history, or access personal folders in order to maintain system integrity and to ensure compliance with responsible use of the Network. Students using the Network acknowledge that the School has the capacity and the right to review histories of Internet sites visited under individual login accounts, and generally log Network access.

MUSIC

- Students may never upload personally sourced music files on to the School network.
- Listening to recreational music files stored on student owned USB's is not allowed during school time for the reason that staff have a duty of care to pre-view audio-visual material for educational appropriateness.
- Class teachers may permit selected school-owned music files to be played to the whole class at the same time.
- Class teachers may request students source music for specific media projects and this will include guidelines on copyright rules.

PHOTOGRAPHY AND VIDEOGRAPHY

School laptops have inbuilt cameras used for photography and videography intended for educational use only.

- Students may not take photos or videos of other students or staff on any device without first seeking their permission and under the supervision of their class teacher.
- Under no circumstances may students 'edit' the photographs of other students or staff.
- Under no circumstances may students 'share' the photographs of other students or staff to the Internet, Intranet, LMS, Network drives, USB's without direct supervision of their class teacher.
- Consequences for Breach of these explicit Policies are outlined below.

STORAGE CAPACITY

Users are expected to remain within allocated disk space. Network servers are not to be used as archival devices or to store personal files. Any Files deemed not to be School related, will be deleted. All student personal spaces will be deleted from the Network at the end of each school year.

The only removable storage media allowed to be used are USB storage devices. All other devices such as SD flash cards, mobile phones, iPods, Minidisks, MP3 players etc. are strictly not allowed without approval prior to each use. SD cards and Flash Drives could be required for a specific course of study such as Applied Information Technology or Design.

No software is to be run from the allowed removable media, nor must any software be used to support the allowed removable media when on the School network. Students are not allowed to store programmes in their allocated H drives, One Drives or USB, or run/ install any programmes on the School computers or network. These drives are only to be used to save and back up school related files and folders.

Data being used in conjunction with the removable storage media must only be School related and must not be used for personal use. Active and audio media files such as mpg, wav, avi etc. are strictly not to be used without permission.

ILLEGAL COPYING

Students are not permitted to download or install any commercial software, shareware, or freeware onto network or local drives or disks. Students should not copy other people's work or attempt to access other students' files.

No material should be accessed, or attempted to be accessed, which is not in line with the School's code of behaviour and if students encounter such material by accident, they must report it to a staff member immediately.

SYSTEM INTEGRITY

Students should not engage in behaviour that will in any way compromise the integrity or security of the network, or individual peripherals running on it. This includes the reconfiguring of workstation settings, disconnecting or re-routing of network cables, unauthorized access to network protocols, and the like. Are we using upper or Lower Case N for Network? This is inconsistent throughout the policy documents.

CONSEQUENCES OF BREACH OF POLICY

The School will investigate all alleged breaches of this policy that are reported to it. The School notes its obligations to report a particular incident that breaches this policy to the Police where it is required to do so. Staff and students of the School and the parents of our students must be aware that in those circumstances where a crime has been committed because of the misuse of Social Media or other technology that they may be the subject of a formal police investigation concerning such misuse. In that event, the School will have no control over the manner and extent of the police investigation.

The School reserves the right to apply all sanctions and implement such procedures as it considers necessary in the resolution of alleged breaches of this policy.

Without limiting the nature of the procedures or sanctions that may be applied, the following may be considered necessary by the School:

- Implementation of a management plan and/or contract of student behaviour;
- Requiring a student and/or students to undertake counselling and/or mediation, and/or delivering apologies and any other form of restorative action as deemed necessary, including, if appropriate, financial compensation to affected parties;
- Removal of certain entitlements and privileges from a student's School programme;
- The application of School detentions;
- A student being placed on formal probation within the School on such terms and conditions as the School considers necessary;
- Requiring a student and/or students to be interviewed together with their parents to discuss the position of a student at the School; and
- The removal of a student from the School on a temporary or permanent basis.

This policy is complementary to all the other stated policies and objectives of the School's student welfare policies and is to be read as a policy that aims to promote an effective and harmonious School environment.

USE OF SOFTWARE AND EXTERNAL DEVICES ON THE NETWORK

The School does not allow the general installation of certain types of external devices on the School Network. This also relates to the software that is needed for these devices to operate as well as any software required on the School Network.

This policy applies to both staff and students. A brief list of some of the devices is below.

Accepted devices for installation

- USB Flash (thumb) drives
- Video Cameras
- Still Cameras (including SLR Digital)

Restricted devices (not owned by the School)

- Mobile Phones, including Smart Phones/Tablets
- Wearable technology (Eg. Smart watches)
- MP3 Players
- IPods
- Personal Laptops and Tablets
- External optical drives/ hard drives

The School reserves the right to indicate to students at any time additional guidelines on those devices that can and cannot be installed on the Network.

If there is a need to have any of the restricted devices installed, you will need to inform the IT Department. Staff members are restricted from installing external devices or software without prior knowledge or approval from the IT Department.

Any software required by staff needs to be divulged to the IT department. When requesting software installation, adequate time must be given to test the software within our network before it can be deployed.

Whenever possible, a copy of the software should be obtained by the staff member involved, prior to purchase, so that testing on our network can be arranged.

The IT department cannot guarantee that all software/hardware will be compatible with the School's Network.

When sourcing software to be used on the network it is preferred that a site licence be obtained. All software to be installed must be licensed to the School.

All licences must be presented to the IT Department at the same time as the request for installation is made.

Software without current licences will not be installed. NO EXCEPTIONS.

LEARNING TECHNOLOGY INTEGRATION PROGRAMME

Advances in information communication technology are changing how schools develop and deliver learning programmes. The Learning Technology Integration Programme seeks to improve student learning outcomes through the integration of technology into teaching and learning.

The School's vision is to utilise information technology to enhance the School's teaching and learning environment; and enable students to become literate, self-directed learners, flexible problem solvers and productive members of a technology-oriented society.

The programme includes use of the School's Canvas Learning Management System (LMS) through which students can access educational material and submit assignments. It is also based on the implementation of a Notebook programme in which all Year 4-12 students are issued with a Notebook computer, for their sole use to complete learning tasks both at School and at home.

Students and parents are required to be aware of and adhere to the appropriate School policies related to ICT use and also the 'LTIP User Guide' and 'LTIP Policy Guide' documents.

NETWORK, INTERNET AND EMAIL ACCEPTABLE USE POLICY

The School's information technology resources are provided for educational (learning and teaching) and administrative activities. Access to resources is provided with the expectation that all users act in a considerate and responsible manner, and adhere to the relevant School policies.

SECURITY OF THE NOTEBOOK

At all times the security of the Notebook is a student's responsibility. Each student will have access to a secure storage locker outside their home classroom at School so that their Notebook may be stored securely when not in use.

Throughout the day, a student's Notebook must be in either of the following places:

- With the student, in supervised use.
- With the student, in the approved carry bag or backpack.
- Apart from the student, in a locked locker,
- Apart from the student, with the IT Help Desk.

What to do in the event of theft or loss of a Notebook at School?

If a student were to lose their Notebook, they would be required to report this immediately to the IT Help Desk and to their class teacher. Notebooks found unattended in open classrooms or on the School grounds are to be taken to the IT Help Desk. Students should immediately report lost Notebooks to the IT Help Desk in order to retrieve lost computers.

What to do in the event of damage to a Notebook?

Damage of any kind to the Notebook should be reported immediately to the IT Help Desk. Depending on the circumstances and the nature of the damage sustained, the Notebook may be covered by insurance.

There are serious consequences if a student is found to be careless, thoughtless, negligent or destructive with either their own Notebook or another student's. For insurance purposes, students should always transport their Notebook in the approved protective case/sleeve.

TRAVELLING OUT OF SCHOOL

Students are expected to take appropriate precautions and care with the Notebook when travelling to and from School. It should be inconspicuous and kept out of sight. If a student travels between home and School by public transport, the Notebook must remain in his / her School backpack or carry bag for the duration of the journey.

TECHNICAL SUPPORT – IT HELP DESK

The School's IT Help Desk, (located on the second floor of the Main Administrative building) will be open on School days from 8:00am–4:00pm, allowing students and staff to seek technical assistance regarding their Notebook computers when necessary.

For further information about the LTIP programme, please contact the appropriate sub-school ICT Co-Ordinator via reception or email;

Mrs Michelle Pestel via mpestel@pmacs.wa.edu.au
Mr Richard Cackett, via rcackett@pmacs.wa.edu.au
Ms Andrea West, via awest@pmacs.wa.edu.au