ST PETER'S COLLEGE

Policy Title	**ACCEPTABLE IT USE POLICY**
Drafting Committee	K Vemer Council Member C MacLeod Council Member
IT Steering Committee	K Vemer Council Member C MacLeod Council Member C Pariola Business Manager R Morais Head S Matthews Deputy Head: Academic S Tudhope IT Director R Buy Independent D Maroun Netology V Mould Independent
Review Requested by	Bi-Annual Review
Recommended by	Executive
Approved by	Council
Date Approved	9 November 2016
Implemented by (Compliance Monitoring)	A Jennings Compliance Manager
Review/Modified date **V1.0** **V1.1** **V1.3** **V1.4** **V1.5** **V1.6** **V1.7**	 July 2016 October 2016 (Updated with legal input) November 2016 (Updated formatting) January 2018 March 2019 October 2019
Rescinded	
Relevant Legislation	South African legislation and case law relating to Social Media
Bibliography	St Peter's College (2016): *New Students Information Booklet.* Fourways High School (9December 2014): *Policy on Safe-Keeping and Security of Devices.*

	Fourways High School: *Device Policy.* Wynberg Girls' High School: *BYOD Policy.* Good TM: *Bring Your Own Device Individual Liable User Policy Considerations.* NSW Government Education and Communities: *Bring Your Own Device in Schools, 2013 Literature Review.* Collegiate Girls' High School: *Information Systems and Social Media Policy.* Burlington High School: *Technology/Network Acceptable Use Policy* Fish Hoek High School: *Computer Education & Acceptable Use Policy* St Mary's Diocesan School for Girls: *Social Networking Policy* St Martin's School Bournemouth: *Computer and Internet Acceptable Use Policy* Wynberg Girls: *Internet Acceptable Use Policy* SANS Consensus Policy Resource Community: *Acceptable use Policy*
Date on Server	

TABLE OF CONTENTS

1. INTRODUCTION

St Peter's College's aim is for students and staff alike to use technology for learning. Technology aids in creative problem solving, and collaboration in today's world. While we want users to be active in today's connected world, we also want them to be safe, legal and responsible.

While IT, the Internet and social media create numerous new opportunities, they also create many new challenges and risks that the school could face. To manage this risk, the use of all IT facilities provided by St Peter's College must be consistent with this policy.

Students, teachers, staff and any IT users are responsible for good behaviour on the Internet just as they are in a classroom or a corridor. Remember that access is a privilege, not a right, and inappropriate use will result in that privilege being withdrawn.

This document forms part of the **BYOD Policy and Agreement** and related documents, and applies to the use of information, electronic and computing devices, and network resources within St Peter's College; or interaction with a third party.

2. PURPOSE

This document serves to:

2.1. Guide the staff and students of St Peter's College to work safely and responsibly with the Internet and other IT technologies and devices. This document is by no means exhaustive but serves to assist in providing information should a user have a specific query on IT usage.

2.2. Ensure safer IT working practice.

2.3. Guide any users, including staff or other adults who work with students of the School within the IT environment.

2.4. Ensure that all staff, students and parents understand and agree with the approach taken to IT.

2.5. Promote the effective use of IT for staff and students at the School.

2.6. Give a clear message that disciplinary or legal actions will be taken in the event of transgressions of the IT policies and guidelines.

2.7. Any exception to the policy must be approved in writing by the Deputy Head: Academics in advance.

3. GUIDING PRINCIPLES

3.1. The School and the management reserve the right to make professional judgments in situations not covered by this policy.

3.2. It is understood that the School is not responsible for monitoring or controlling the data, e-mail or other communications of individuals utilising the network; but network administrators have the right to review files and communication as they see fit, to maintain system integrity and responsible use. In other words, files within the St Peter's College online environment are not to be regarded as private.

3.3. The School will only intervene in out-of-school activities if it is in the best interest of the Student or if the Student's behaviour brings the School's name into disrepute.

3.4. All IT users are expected to exhibit responsible IT user citizenship.

3.5. The policy covers end-user IT groups, as well as free-standing devices which are autonomous.

3.6. Respect yourself: Consider images and information that you post online.

3.7. Protect yourself: Do not publish your personal detail, contact detail or schedule of activities.

3.8. Respect others: Do not use technology to bully or tease other people.

3.9. Protect others: Report misuse and abuse. Do not forward inappropriate information.

3.10. Respect intellectual property: Suitably cite any use of websites, books, media, etc.

3.11. Protect intellectual property: Appropriately request the use of software and media that others produce.

3.12. Respect resources: Do not affect security breaches or disrupt network communication, but use the Internet and email for study or for school authorised/supervised activities, but at all times for educational purposes.

3.13. Protect resources: Ensure proper security and access measures are in place.

3.14. Respect assets: Take responsibility for looking after your own and the School's IT devices.

3.15. Protect assets: Ensure that you take precaution with your and the School's IT devices with regard to passwords, backups, virus protection and physical location.

3.16. The use of any device or IT facilities may not in any form violate any South-African legislation or regulations. Users will comply with School standards and will be held liable to the agreements they have signed. These guidelines have been established to avoid disagreements and any potential litigation.

4. ACCEPTABLE IT USE

4.1. All users are responsible for exercising good judgment regarding appropriate use of IT devices and information, and network resources in accordance with any South-African legislation or regulations. Users are to comply with School standards and honour the agreements they have signed.

4.2. The St Peter's College network is to be used in a responsible and legal manner. Users are expected to use the Internet for the following purposes:

- Educational purposes; and
- Constructive communication with other Internet users.

4.3. Users should regard participation in online media as an extension of their classrooms or School grounds and anything which is permitted in a formal classroom is acceptable online, and anything which would be unacceptable in a classroom should also be unacceptable online.

5. UNACCEPTABLE IT USE

5.1. Violations of the IT policies and guidelines will be dealt with according to the guidelines in the **Code of Conduct and Disciplinary Procedure**, and may result in the loss of access to the network as well as disciplinary or legal action.

5.2. Where users are associated with the School and are engaged in an inappropriate fashion, the School can intervene to prevent reputational damage to the School. Such abuse of the media could result in disciplinary action.

5.3. Parents must accept their roles in managing the private activities of their children. They should not expect the School to police the private and out of school IT and Internet activities of Students of the School; but the School might choose to intervene in such situations, if it is in the best interests of the Student and/or School to do so.

6. RESPECT YOUSELF

6.1. Users are expected to demonstrate appropriate and responsible behaviour at School and outside of School when using their IT devices.

6.2. Remember that the use of social media in schoolwork (either in classrooms or outside) is an extension of the classroom and anything that is acceptable in class is acceptable online and anything that is unacceptable in class is unacceptable online. Social media is a public platform and the rules of society count on social media, just as in real life.

6.3. How you represent yourself online is an extension of yourself. You create your own on-line image, ensure that it is in line with how you want other people to see you. Do not misrepresent yourself by using someone else's identity, or create a fictional persona.

6.4. Be responsible for whatever you write. Be aware of what you post online. Social media venues are very public. What you contribute leaves a digital footprint for all to see. Do not post anything you wouldn't want friends, enemies, parents, teachers, or a future employer to see.

6.5. Ensure that appropriate and proper grammar and punctuation are applied when writing anything for online posting. Be professional.

6.6. Do not try and hide your identity when sending emails or using any other IT facilities.

6.7. Privacy on the School Internet

6.7.1. Files stored on School computers or network domain are not private. The School has the right to inspect, copy of review any information stored on the school's OneDrive account.

6.7.2. Do not send any private information that you would not want to be made public.

7. PROTECT YOURSELF

7.1. Be careful of what you post online as it is an extension of yourself. Social media is by its' very nature public, and information can be shared with other people via their friends and/or contacts. Take appropriate care when using social media.

7.2. Ensure that you have adequate profile security and privacy settings.

7.3. Do not post any confidential information about yourself, the School, teachers, Students or any other member of the community on social media platforms.

7.4. Never tell anyone you meet on the Internet your home address, your telephone number, any details about the School, or send them your picture. Be cautious about providing any personal details to anyone that you do not know face to face.

7.5. Do not agree to meet anyone you have met online, without your parent's approval.

7.6. If you are the recipient of any cyber bullying or abuse, keep a record of this, and report it to your register teacher or Grade Head.

7.7. If you have received a message that is inappropriate or makes you feel uncomfortable, disclose this to your register teacher or Grade Head. Do not forward this message or spread it in any way to the community.

7.8. Teachers and students who are still at School should not befriend one another on Facebook or other social media, except in the case of a site specifically set up for professional purposes. Staff should not befriend ex-students where siblings continue to attend the School. Instances can occur where the teacher and student are part of the same social circle and this needs to be communicated to the Grade Head.

7.9. Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which could destroy information and software on the computers.

7.10. Ensure that communication takes place within clear and explicit professional boundaries.

7.11. Staff are to use their School e-mail address and not their private e-mail address for all official communication.

7.12. Passwords

7.12.1. Passwords and/or other access detail are to be kept confidential and used only by the user to whom they belong.

7.12.2. The use of a "lock password" is compulsory.

7.12.3. Create a strong password that consist of a combination of upper and lowercase letters, numbers and symbols.

7.12.4. Change your password regularly.

7.12.5. If you suspect that your password has been hacked, change it immediately.

7.12.6. You will be advised on how to change your password by the IT representative.

8. RESPECT OTHERS

8.1. Adhere to the values and ethos of the School, especially in situations where you may be associated with the School.

8.2. Understand that you are an ambassador of the School in all online activities. Material published on social networking websites should not reflect negatively on fellow Students, educators, or on St Peter's College. You will be held responsible for how you represent yourself and your School on the Internet.

8.3. Do not post any confidential information about other people, the School, colleagues, Students or any other member of the community.

8.4. Do not post any false information about other people, the School, colleagues, Students or any other member of the community.

8.5. Do not abuse confidential or any privileged information accessed through private social networking media.

8.6. Staff, Parents or Students should not abuse any privileged or confidential information they might have access to in any way in private social networking media.

8.7. Do not forward a message that was sent to you privately without the permission of the person who sent you the message. You may not use any other user's account or access any other user's files.

8.8. Do not record teachers or any adult without their permission.

8.9. Do not engage in cyber bullying, insulting, racial or sexual language, derogatory or offensive comment as this is unacceptable and not in line with St Peter's values and norms.

8.10. Do not post inappropriate material (e.g. pornography) as it will lead to disciplinary action.

8.11. Post what you want your teachers, colleagues, fellow Students and Parents to see.

8.12. Do not discuss other Students, teachers or staff on social media.

8.13. Should you not be in agreement with the School about a particular matter, do not criticise the School and its policies on public forum, but instead use the School's formal channels for this.

8.14. Where there is a possibility that you may be associated with the School, you should act in a manner which is consistent with the general philosophies and values of the School, and does not bring the School into disrepute.

8.15. In the Classroom

8.15.1. All devices are to be used for educational purposes only during lesson time.

8.15.2. The device may not be used to communicate with each other; type emails or play games on during lesson time.

8.15.3. Sound must be muted at all times.

8.15.4. Listening to music during class is not permitted, unless it has been allowed by the teacher.

8.15.5. Device malfunction is not an acceptable excuse for not submitting work.

8.15.6. It is the user's responsibility to ensure that devices are charged and ready for use in the classroom.

9. PROTECT OTHERS

9.1. Users must understand that the School filters and restricts access to certain sites and data that is deemed either private to certain groups, or inappropriate or illegal material.

9.2. If you run across inappropriate material that makes you feel uncomfortable, or is not respectful, report this to your register teacher or Grade Head right away. In the case of staff, these reports should be made to the Deputy Head: Academics.

9.3. If any person inadvertently accesses any website containing offensive material such person must immediately report this to the Head: Academics, so that the site can be blocked.

9.4. If you are aware that someone that you know is being continuously harassed via any IT facilities, report this to the register teacher, Grade Head, or staff to the Head: Academics.

10. RESPECT INTELLECTUAL PROPERTY

10.1. Do your own work, don't be guilty of plagiarism. Plagiarism is using someone else's ideas or words as your own. This goes for graphics, poems, photographs, music or text. Give credit where due for any use in assignments or other documents.

11. PROTECT INTELLECTUAL PROPERTY

11.1. Ensure that the correct approval has been obtained before downloading or copying any material.

11.2. If you become aware of any attempt or use of others' intellectual property, report this to your register teacher.

12. RESPECT RESOURCES

12.1. Restricted On-line access

12.1.1. Users are prohibited from attempting to access any IT facilities, software or data which they have not been authorised to use.

12.1.2. Users may not modify computer files, folders or settings on any of the School's IT facilities, without proper written permission.

12.1.3. You may not make any deliberate attempt to disrupt the computer system or destroy data by spreading computer viruses or by any other means.

12.1.4. Accessing or intentionally destroying software or licensed software in a computer facility without the permission of the owner of such software or licensed software or the controlling authority of the facility, is deemed inappropriate.

12.2. Internet Usage

12.2.1. The Internet should only be used for study or for School authorised/supervised activities.

12.2.2. Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.

12.2.3. Do not engage in 'chat' activities over the Internet, or use the Internet to play games. This takes up valuable resources which could be used by others to benefit their studies.

12.2.4. Students are not permitted to use the School Internet to access social media such as Facebook.

12.2.5. Do not intentionally waste resources by storing large amounts of data on the network; or by downloading large amounts of data, music, apps or similar.

12.2.6. Use of the School computing network is not for commercial or excessive private purposes.

12.3. School Email, database and advertising

12.3.1. You will not post chain letters or engage in spamming. Spamming is sending a message to a large number of people.

12.3.2. The School email database is not to be used by any user without explicit approval by the School's Marketing Department.

12.3.3. Any promotional material must be submitted to the HOD/MIC and Marketing for approval, prior to publication.

12.3.4. Promotions may be posted on the School Facebook page only once approved by the Moderator.

12.3.5. Other IT facilities such as the Keyhole or Communicator, may only be utilised for promotions once written approval has been obtained from the HOD/MIC and the School's Marketing Department.

12.3.6. Postings must be kept legal, ethical, respectful, and as brief as possible.

13. PROTECT RESOURCES

13.1. If you become aware of any attempt or abuse of resources, report this to your register teacher.

14. RESPECT ASSETS

14.1. Damaging any computer equipment is not permitted.

14.2. No food or drink is to be placed on or near any computer devices.

14.3. No smoking is permitted near any hardware device.

14.4. Do not subject the device to direct sunlight; extreme heat or cold.

14.5. Do not drop the device; or drop anything heavy onto the device.

14.6. Keep the device away from all magnets.

14.7. Users are responsible for keeping their device up-to-date and secure.

14.8. Users are responsible to charge, backup and update their devices.

14.9. Users are responsible to have any broken devices fixed. This is not the responsibility of the School.

14.10. Do not make unauthorised copies of licensed software.

14.11. Do not load unauthorised software onto computer facilities.

15. PROTECT ASSETS

15.1. Access to the School's Resource Centre and Computer Room will only be during school hours.

15.2. Immediately report any damage or faults involving equipment or software, however this may have happened.

15.3. No hardware or software owned by the School may be removed from the School premises without written permission.

15.4. Vandalism is defined as any malicious attempt to harm, modify, or destroy equipment or data of the School or another user. This includes, but is not limited to, the transferring or creating of computer viruses. Any malicious use of any IT equipment will be treated as a violation of this policy, and appropriate action taken.

15.5. Users bring their own property to the School at their own risk, and are responsible to look after their own devices at all times. All Students have been allocated a locker, where they can store their device when not in use.

15.6. Refer to the section under **BYOD Requirements** on anti-virus software and insure that this is installed.

15.7. Passwords and/or other access details are to be kept confidential and used only by the user to whom they belong. The use of a "lock password" on your device is compulsory.

15.8. The user must ensure that they do regular backups of their device and any locally installed applications or data.

15.9. Parents/guardian or owners are responsible for adequately insuring any device brought onto the School property.

16. A FINAL NOTE

The use of any device or IT facilities may not in any form violate any South-African legislation or regulations. Users are to comply with the School standards and honour the agreements they have signed. By using St Peter's IT facilities, the user automatically agrees to have read and understood the above and agrees to use the School IT systems (both in and out of School) and their own devices (in School and when carrying out communications related to the School) within these guidelines.