IN FUTURUM FORTITER

ST PETER’S
COLLEGE

BRING YOUR OWN DEVICE POLICY AND AGREEMENT

TABLE OF CONTENTS

1. TERMINOLOGY

1.1	The School	St Peter's College
1.2	Student	Any current Student at St Peter's College
1.3	Parent	The Parent or legal guardian of a Student
1.4	User	Any person using or accessing any of the School's IT facilities
1.5	BYOD	Bring Your Own Device (a technical solution where users bring their own device to school to access the Internet)
1.6	IT	Information Technology

1.7 IT Devices (this list is not exhaustive and may be added to in the future):

- Computer hardware device (IPAD, tablet, notebook, printer)
- Internet
- Electronic device such as digital cameras and scanners
- Email
- Accompanying software
- SMART board (interactive white board)
- LCD Projector
- Video conferencing
- Smart phone

2. INTRODUCTION

Technology has changed the landscape of learning, with unlimited access to digital content, resources, expertise, databases and communities of interest. St Peter's College ("**SPC")** integrates technology into the curriculum, and empowers Students and staff with access to the School wireless network through a personal device.

As part of the curriculum, St Peter's College requires each Student to bring a personal device to the classroom. All Students and Parents/guardians, or staff that use a BYOD, need to understand and agree to the BYOD (Bring Your Own Device) Agreement. The acceptance of the agreement does not have to be re-submitted every year, only in instances where major changes have been made to the agreement.

In addition, all Students and Parents/guardians, staff or any other BYOD users need to read, understand, and agree to adhere to the information and responsibilities stated in the

Code of Conduct and Disciplinary Procedure;

Acceptable IT Use Policy;

BYOD Requirements; and the

New User Leaflet.

These policies can be found under Resources on the School Communicator and website. Users are required to indicate their acceptance of the above policies and procedures by means of an electronic acceptance at every sign-in to the SPC network.

Users will be expected to comply with all class and School rules while using personal devices, or accessing the School IT facilities. It is a privilege to have access to the wireless network and users not complying with the conditions contained in this policy will be denied access for a period of time, and may face further disciplinary or legal actions.

3. PURPOSE

Through BYOD the School aims to promote the effective use of IT to staff and Students by creating a more collaborative school culture and providing different ways of accessing information and communicating with people. The School believes that Students and staff alike should be encouraged to develop their academic and technological skills through these powerful tools and resources, and aims to extend student learning, develop digital literacy, self-directed learning, provide interactive feedback about student performance, and promote good IT citizenship for users, which will prepare them for the high-tech world in which they will live, learn and work.

This document serves to

3.1 Act as a reference point for staff, Students, or any users of St Peter's College IT facilities, detailing resources available;

3.2 Ensure that all staff, Students and Parents/guardians understand and agree with the approach taken to IT by the School;

3.3 Regulate end-user IT groups as well as free-standing devices which are autonomous; and to

3.4 Ensure that all users follow the policies and procedures as recorded herewith. These guidelines have been established to avoid any potential disagreements.

4. PROCEDURE

4.1 Each eligible user is provided with a username with access to the SPC network. They are further given a Google-based St Peter's College email address and access to Google Classroom.

4.2 Starting with Grade 8 in 2016 all students are to use laptops as part of their every-day learning experience. This strategy is an effective implementation of BYOD.

4.3 The School provides access to the IT infrastructure to all Students during the school peak hours as well as after hours.

4.4 Access to the Resource Centre and Computer Room is made available during school hours.

5. GUIDING PRINCIPLES

5.1 Eligibility and Restrictions

5.1.1 All users, irrespective of ability, gender or race, have equal opportunity to access and utilise the IT infrastructure.

5.1.2 All users are offered an equitable educational experience by having access to the same materials and learning opportunities.

5.1.3 Access to network services is given to users who agree to act in a considerate and responsible manner. Access is a privilege, not a right.

5.1.4 Users will comply with the School standards and honour the agreements they have signed.

5.1.5 The School respects the individual privacy of users. However, the School may at its own discretion examine, move or delete files, including electronic mail (e-mail), for purposes of system maintenance or if the files are determined to be disruptive to the system or its users, either intentionally or unintentionally.

5.2 Policy Violations

5.2.1 The School may examine any device as defined in the **Acceptable IT Use Policy** that is suspected of causing technology problems or was the source of an attack or virus infection.

5.2.2 Devices may be subjected to search by school administrators (School Executive, Management, HOD, register teacher) if the device is suspected of a violation of the School's Code of Conduct. If the device is locked or password protected, the user will be required to unlock the device at the request of a school administrator.

5.2.3 Violations will be dealt with accordingly, and may result in the loss of access to the network, as well as disciplinary or legal action.

5.3 Reimbursement

5.3.1 No users are ever eligible to be reimbursed by SPC for any device purchases, Internet usage or any other IT use.

5.4 Internet Connectivity

5.4.1 The School strives to provide the best possible IT services and internet access, but does not guarantee uninterrupted connectivity or the quality of connectivity. The quality of Internet coverage may vary in different areas around the School. Each user needs to act responsibly when accessing the Internet.

6. HARDWARE AND SOFTWARE REQUIREMENTS

The School recommends the use of laptops, with Windows as an operating system, and using the Google Classroom and Microsoft Office platforms.

For detail on device requirements, refer to the **BYOD Requirements** document.

7. GETTING STARTED

Please refer to the **New User Leaflet** to get started.

8. RESPONSIBILITIES

8.1 It is the responsibility of the user to ensure that they act in a manner which would be deemed appropriate for good digital citizenship, and comply with the specified guidelines set out in this policy. Further guidelines on user responsibility, classroom behaviour, and social media may be found in the **Acceptable IT Use Policy**.

8.2 Users are responsible for good behaviour on the computer network, just as they are in classrooms and on the College grounds. Users are expected to conduct themselves appropriately at all times and use the Internet and email facilities responsibly.

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

8.4 Users are responsible for keeping their device secure.

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

9. SECURITY AND SAFETY

It is emphasised that each user should take all necessary steps to minimise the risk of losing any device, personal applications or data. Refer to the **Acceptable IT Use Policy** for further information on security, safety, and social media.

9.1 Physical location of devices

9.1.1 Users are responsible to look after their own devices.

9.1.2 Staff devices need to be secured with a cable lock when in use.

9.1.3 All Students have been allocated a locker, where they can store their device when not in use.

9.1.4 All locker areas have been fitted with camera surveillance.

9.1.5 Students need to purchase a lock for this locker, which can be obtained from the School Shop.

9.1.6 Each locker has a built in two-prong electricity plug point from which the device can be charged.

9.2 Viruses

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

9.3 Passwords

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

9.3.2 Refer to the **New User Leaflet** for further information on setting your password.

9.3.3 The use of a "lock password" on your device is compulsory.

9.4 On-line Access

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

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

9.5 Data backup

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

10. Liability for loss

10.1 Users bring their own property including any devices to the School at their own risk.

10.2 The School will not be held liable for loss or damage of any personal device, application or data, whether directly or indirectly resulting from the usage of School applications or data, and/or the wiping of such applications or data, or the whole device.

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

11. USER AND DEVICE SUPPORT

11.1 The user is fully responsible for their own device and any hardware or software malfunctions thereof should be resolved by the user themselves. The IT department is not responsible for maintaining or troubleshooting BYO devices.

11.2 Parents/guardians or owners of devices must pursue queries with the supplier where the device was purchased or independent device specialists.

11.3 Should users experience problems with Google access, they should contact their register teacher.

12. QUESTIONS AND ASSISTANCE

For assistance with BYOD or learning-related questions, please contact the

Deputy Head: Academics Mrs Shelley Matthews matthewss@stpeterscollege.co.za

13. ACCEPTING THE AGREEMENT

Kindly ensure that you submit either the relevant **STUDENT AND PARENT/GUARDIAN DECLARATION** or the **STAFF DECLARATION** to the School**.** The declaration will be submitted electronically to the School.