VICTORIA PARK HIGH SCHOOL

PREPARED FOR LIFE

Device Policy

(This policy needs to be initialled on each page, with full signature on the last page

by the Student and Parent / Guardian)

Policy Number	*VPHS KP021*	Authorised By	Authorised By
Date	**Revision**	**SGB Chairperson**	**School Principal**
2018-11-18	0		

Device Policy

1 PREAMBLE

1.1 Victoria Park High School has introduced a **"BYOD"** (Bring Your Own Device) initiative with effect from January 2019. This policy is intended to cover relevant aspects of that initiative and may be subject to amendment in the future.

2 DEFINITIONS

2.1 **BYOD** ……… Bring Your Own Device

2.2 **Device** ……. Student's own IPAD or TABLET.

2.3 **ICT** …………. Information Communication Technology.

2.4 **School** …… Victoria Park High School.

2.5 **Student** .... Student of Victoria Park High School.

2.6 **User** ………. Any person using or accessing any of the School's ICT facilities

3 RESPONSIBILITY

3.1 Students are expected to demonstrate appropriate and responsible behaviour when using the School's ICT facilities as well as when using their own personal Devices.

3.2 Students are expected to comply with the specified guidelines and rules set out below. Necessary disciplinary action will be taken against Students who disregard this policy.

3.3 Students bring their Devices to use at Victoria Park High School at their own risk.

3.4 Students are personally responsible for keeping their Device up-to-date and secure.

3.5 Victoria Park High School is in no way responsible for:

- Maintenance of any Device.
- The loading, charging, back-up, updating of apps etc.
- Broken Devices.
- Lost or stolen Devices.

4 TERMS AND CONDITIONS

4.1 The use of any Device and/or the transmission of any electronic material in any form that is in violation of any South African legislation or regulations as well as International Law or any of the School's rules is strictly prohibited. This includes, but is not limited to, copyright material, threatening, obscene or offensive material, or material protected by trade secret.

4.2 The use of the School's ICT facilities is a privilege and not a right. Abuse of such facilities will result in the withdrawal of access from all ICT facilities.

4.3 Students are personally responsible for their actions in accessing and utilising the ICT facilities of the School.

5 MONITORING

5.1 All activities utilising the School's ICT facilities are monitored and logged.

5.2 The School reserves the right always to determine whether usage of the School's ICT facilities is appropriate. This includes the right to review, amongst others, Internet usage, material held in user accounts and server space.

5.3 In reviewing and monitoring user accounts and file server space, the School will respect the privacy of the user accounts always.

5.4 The School reserves the right to inspect any Device and take the appropriate disciplinary action in the event that either the Device or any material contained on the Device, has been or is intended to be used for, any illegal or unlawful activity.

6 INTERNET ACCESS

6.1 Learners will be granted limited access to the Internet via the School's Wi-Fi network.

6.2 Access to Social Networking Websites (e.g. Facebook, Twitter, WhatsApp, Telegram, Instagram, Myspace etc) is not permitted through the school's network.

6.3 Access to online school e-mail services is permitted. However, e-mail services must not be used to download, upload or transfer files that are otherwise restricted, prohibited or contain any offensive or illegal material.

7 SECURITY

7.1 Each Student will be issued with a unique and specific password and/or other access details for each ICT system at the School that they are permitted to access.

7.2 Passwords and/or other access details are to be kept strictly confidential and are to be used only by the Student to whom they were issued.

7.3 No Student may attempt to use any password or other access details belonging to any other person to access any of the School's ICT facilities.

7.4 Students are prohibited from attempting to access any files, folders or similar which they have not been authorised to access.

7.5 Students must not attempt to, nor gain any unauthorised access to any of the School's ICT facilities or systems for any purpose. Such hacking or attempted hacking is a criminal offence under the Electronic Communication and Transaction Act, Act 25 of 2002. Any attempt to access any of the Schools ICT facilities posing as 'system administrator' will result in cancellation of User privileges and the implementation of disciplinary procedures against that person.

7.6 No Student may use another Student's account.

7.7 No passwords may be shared amongst Students.

7.8 Students may not modify computer files, folders or settings on any of the Schools ICT facilities without prior authorisation from an IT staff member.

8 ILLEGAL ACTIVITIES

8.1 Pupils must not, by using any of the School's ICT facilities, possess or transmit any illegal material of any nature or form. (Note - As the internet is global, some activities/material which may be legal in other countries, may be illegal in South Africa and vice versa).

9 REGULATIONS

9.1 Misconduct in relation to the usage of ICT facilities could result in the person who performed such misconduct being legally prosecuted for a variety of criminal offences, or being subjected to a civil claim for damages, or both.

9.2 **Examples of such infringements are:**

9.2.1 Infringement of a person's constitutional rights to dignity, respect, privacy etc. Subjecting a person to "Hate Speech" or racist comments.

9.2.2 Illegal access to information

9.2.3 Illegal interception of communication

9.2.4 Harassment

9.2.5 Slander

9.2.6 Defamation

9.2.7 Fraud & Corruption

9.2.8 Extortion

9.2.9 Copyright & Plagiarism

9.3 Sexual and pornography offences. In relation to a breach by or against a Student of any of the above, the School, its employees, parents and Students have a legal obligation to report it to the authorities. Failure to do so could constitute a criminal offence.

10 OFFENSIVE MATERIAL

10.1 If any person inadvertently accesses any web-site containing offensive material such person must immediately report it to the IT Service Desk, so that the site can be blocked.

10.2 Under no circumstances must the name or URL of the site be disclosed to other Students or Staff.

10.3 Any person found attempting to access, or to be in possession of, offensive material, will have their Wi-Fi and Internet access blocked, and in addition, will be subjected to the School Disciplinary Process.

10.4 It is a criminal offence, even for a child, to create, download, possess, distribute or display any child pornography.

10.5 It is also a criminal offence to display or distribute any pornographic material to any child even if the person displaying or distributing such pornographic material is a child themselves.

11 CYBER BULLYING

11.1 Cyber bullying is illegal and is strictly prohibited.

11.2 Cyber bullying occurs when any person is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another person using any form of ICT facility.

11.3 Any person who is subjected to cyber bullying must report it immediately to their Grade Head or a Deputy Principal.

11.4 Any person who is aware that another person is engaging in, or is the target of cyber bullying, must report it immediately to their Grade Head or a Deputy Principal.

11.5 Examples of cyber bullying are contained in **Annexure A**. Note that this is not an all-encompassing list and other actions may also constitute cyber bullying

12 CLASSROOM PRACTICE

12.1 All Devices are to be used for educational purposes only during lesson time.

12.2 If a Device is left at home or is not charged, the Student remains responsible for completing all schoolwork as if they had use of their Device. This will be punished according to the School Discipline Procedures.

12.3 Students are responsible for ensuring their Device is fully charged before the start of the School day.

12.4 Devices should be brought to School each day unless a Teacher instructs otherwise.

12.5 Sound must be muted at all times unless permission is obtained from the Teacher.

12.6 Games are not to be played during any curriculum activity.

12.7 Students must ensure that they do not lose work due to mechanical failure or accidental deletion. Device malfunctions are not an acceptable excuse for not submitting work. Teachers and the IT department will instruct Students on methods of managing workflow.

12.8 Use of Devices during the school day is at the discretion of Teachers and Staff. Students must use Devices as directed by their Teacher.

12.9 The use of a Device is not to be a distraction in any way to Teachers or Students and may not disrupt teaching in any way.

12.10 Students may not use their Devices to communicate with each other during class time, such as email, chat messaging and similar.

12.11 Students should always turn off and secure their Device after completing their work to protect their information.

12.12 The use of a “lock” password is compulsory.

13 GENERAL

13.1 Any Student who attempts to hack or interfere with any other account, including any attempt to break into the network, spread viruses or change any directory permissions will be permanently denied access to the School's Wi-Fi and will be subjected to the School's disciplinary process as well as a criminal case possibly being opened against them.

13.2 Students are prohibited from attempting to bypass blocked sites by any means whatsoever. Any such attempt will result in the Student being blocked from the school's Wi-Fi network and subjected to the School's Disciplinary process.

13.3 No printing is allowed at the school. Learners may pay for printing services in the CAT Labs.

13.4 No Student is permitted to download or copy any copyrighted or otherwise protected material onto their Device.

13.5 Students may not play games or watch videos via the Internet.

13.6 Using offensive language when transmitting to any other Student or a member of the School's Staff is prohibited – this includes impolite, anti-social, profane, abusive, racist, or sexist language.

13.7 Students must not use their Device's camera to take images/videos of any Student or Teacher that may be deemed to be inappropriate in any manner. Doing so may expose the Student taking such images/videos to criminal or civil action.

13.8 Inappropriate media may not be used as a screensaver or background on any Device, including pornographic images, pictures of violence, inappropriate language, alcohol, drug, racist or gang related symbols or pictures.

13.9 Using the Device listen to music in class or whilst walking around the school is forbidden.

13.10 Images or movies of people are not to be shared in a public space on the Internet, without the permission of the individual concerned or a staff member.

13.11 If a Student logs on to IT School Innovation (ITSI) Server with a login that is not your own, your tablet will be denied access for a certain period of time.

13.12 No Teacher or Councillor will take responsibility for the security or charging of the Device.

13.13 No Device may be opened or used during Assembly.

13.14 No Device is to be brought to School on the day of an examination.

13.15 Should any person outside the School access the School's network via a Student's login details, the relevant Student will be suspended from the Wi-Fi pending a Disciplinary Enquiry and the School will open a criminal case against the guilty party.

13.16 Devices belonging to other persons are not to be tampered with in any manner. Any Device found unattended must immediately be handed in at Reception or the IT head.

14 MISUSE OF ICT

If a Student continues to disregard the rules contained in this Policy after one warning, the following will apply.

- Parents will be notified
- Access to the Wi-Fi network will be denied to the Student.
- The Device will be confiscated and placed in the front office for parents to collect.
- The Student will be banned from using a Device at School for a period of time commensurate with the severity of the offence.
- Detention or Community Service will be implemented.

Signed at Port Elizabeth on the ……………. day of ……………………………………. 2019

As Witnesses:

Student Signature …………………………………………………. Student Name ……………………………………………

Parent / Guardian Signature …………………………………… Parent / Guardian Name …………………………..

Please take note of the Annexures A and B

ANNEXURE A
CYBER BULLYING

Examples of Cyber Bullying

- Repeated e-mails or Instant Messages (IM) sent
- Following a person online, into chat rooms, favourite Web sites, etc.
- Building fake profiles, Web sites or accessing another person's e-mail or IM
- Issuing statements to provoke third-party stalking and harassment
- Signing a person up for porn sites and e-mailing lists and junk e-mail and IM.
- Breaking into any person's online accounts.
- Stealing or otherwise accessing a person's passwords
- Posting any image of a person online.
- Posting real or doctored sexual images of any person online
- Sharing personal and/or intimate information about a person online without their permission
- Encouraging the inclusion of any person on any derogatory "hit lists" such as, but not limited to, "ugly lists", "slut lists" and similar.
- Posting or encouraging others to post nasty comments on a person's blog.
- Hacking a person's computer and sending a person malicious codes.
- Sending threats to or attacking others, including while posing as another person.
- Copying others on a person's private e-mail and IM communications.
- Posting bad reviews or feedback on a person without cause.
- Registering a person's name and setting up a bash Web-site or profile.
- Posting rude or provocative comments while posing as another person.
- Sending spam or malware to others, including while posing as another person.
- Breaking the rules of a Web site or service while posing as another person.
- Setting up any "vote" (e.g. "hot or not?") designed to embarrass or humiliate any person.
- Masquerading as another person for any purpose whatsoever.
- Posting any person's contact details online to encourage abuse or harassment or other prejudice to that person.
- Launching a denial of service attack on any Web-site
- Sending "jokes" about a person to others or mailing lists

ANNEXURE B
DEVICE CARE

The following general guidelines are recommended:

- Use protective covers/cases.
- Never drop or place heavy objects on top of the Device. Do not “bump” the tablet against lockers, walls, car doors, floors, etc as it will eventually break the screen.
- Use a soft cloth to clean the Device screen.
- Do not subject the Device to extreme heat or cold.
- Do not leave the Device in the sun.
- Do not place anything in the carrying case that will press against the cover.
- Do not drop the Device.
- Keep the Device away from all liquids
- Keep the Device away from all magnets