TECHNOLOGY POLICY

(23 August 2019)

For the sake of clarity, this Policy is subject to the School's Code of Conduct and any transgressions of this Policy will be dealt with in accordance with the Code of Conduct.

Save to the extent that a term is specifically defined in this document, any defined term shall bear the meaning ascribed to it in the Code of Conduct.

1. Applicability of this Policy

1.1. This Policy applies to any and all usage by School Pupils and staff ("Users"), in whatsoever manner of the following:

1.1.1. the School's internet network, including but not limited to their WiFi network, cloud drives, storage systems and/or hardware servers ("the Network");

1.1.2. any school computer;

1.1.3. any school tablet;

(jointly the "School Assets");

and

1.1.4. any cellphone, laptop, tablet or other mobile communication system owned by a User in their private capacity, **but used on the School's premises** irrespective of whether same is being operated using the School's network or not ("Personal Electronic Devices").

2. Introduction

2.1. The School believes in the value of technology as an educational resource. The School is therefore pleased to be able to offer Users access to the School Assets, as well as the ability to use their own Personal Electronic Devices, subject to the terms of this Policy.

2.2. The Users recognize and accept that School Assets are provided to facilitate teaching, learning and administrative activities at the School and are to be primarily used for this purpose.

3. Rules Regulating the Usage of the School's Assets and/or Personal Electronic Devices:

3.1. General

3.1.1. The use of the School's Assets is a privilege, not a right, and may be revoked if abused.

3.1.2. Users must obtain permission before using the Schools Assets.

3.1.3. Users must treat the School's Assets with care, abiding by the rules of the computer laboratories and libraries which have been, and will be from time to time, communicated in writing and /verbally.

3.1.4. No User may change the operating system settings or any program settings or introduce any code or change to any part of the operating system without explicit written permission of the SABJE system administrator.

3.1.5. No external storage device may be inserted to any part of the system / network without express permission of the SABJE system administrator or the staff member in charge at the relevant time.

3.1.6. No disks, manuals or computer equipment may be removed from any office, computer room, laboratory or library without express written permission of the SABJE system administrator.

3.1.7. Users may only use the facilities of the computer laboratories under the supervision of the appropriate staff members.

3.1.8. Information (text or graphics) may only be printed when it is required for specific School work and with prior permission of the relevant staff member.

3.1.9. Users must ensure that they log off from their workstations when they have completed their work or wish to terminate their approved sessions.

3.1.10. Users may only use their own individualized passwords when accessing and utilizing the Schools Assets and may not for any reason use another party's password at all.

3.2. **Prohibited Usage**

3.2.1. **Content not related to School activities –** Users are not permitted to use the Network for non-school related activities, especially those which are bandwidth intensive, including but not limited to, gaming or downloading or streaming of large audio or video files;

3.2.2. **Content in Violation of the Code of Conduct** – Users shall not use the School Assets or Personal Electronic Devices to intentionally access, share, copy or create material that violates the School's Code of Conduct;

3.2.3. **Content which Constitutes "Banned Content" (as set out in the Social Media Policy)** - Users shall not use the School Assets or Personal Electronic Devices to Publish any Banned Content;

3.2.4. **Content in Violation of the Constitution of the Republic of South Africa** – Users shall not use the School Assets or Personal Electronic devices to intentionally access, share, copy or create material that violates the Constitution of the Republic of South Africa, including but not limited to any content which could be construed to constitute hate speech, including content that is racist, sexist, homophobic or otherwise discriminatory;

3.2.5. **Inappropriate Material –** Neither the School Assets nor any Personal Electronic Devices shall at any time be used to request, share, view or store any content that is obscene, graphic, violent or indecent, including any pornography or other explicit content, as judged in the sole discretion of the School;

3.2.6. **Illegal Content –** Neither the School Assets nor any Personal Electronic Device shall at any time be used to request, transmit or store content that is defamatory, fraudulent or otherwise unlawful, including content that requests, encourages or provides instructions for criminal activities. Content relating to, or in furtherance of, illegal activities will be reported to the South African Police Services;

3.2.7. **Bullying and Harassment –** the School does not tolerate bullying. Neither the School Assets nor any Personal Electronic Device shall at any time be used to engage in conduct that causes or could reasonably be expected to cause, *inter alia*, mental, psychological, physical or emotional harm to any person (whether a Pupil of the School, or not), or which inspires the reasonable belief that such harm may be caused. This includes content that is insulting, harassing, threatening or abusive. This is more fully expounded upon in the School Social Media Policy and Anti-Bullying Policy;

3.2.8. **Spam -** Neither the School Assets nor any Personal Electronic Device shall at any time be used to transmit promotions, advertising, contests, chain letters, or other unrequested material that is designed or likely to cause annoyance, irritation or inconvenience ("Spam");

3.2.9. **Intellectual Property –** Neither the School Assets nor any Personal Electronic Device shall, at any time, be used to infringe the copyright, trade-mark or other intellectual property rights of any person or organisation. In particular, they may not be used to access, download, store or transmit music, videos or other content in violation of the intellectual property rights of any other party;

3.2.10. **Impersonation –** When accessing and/or using the School Assets or Personal Electronic Devices, Users are not permitted to use other's usernames, disguise their identity, impersonate other Users, or send 'anonymous' emails;

3.2.11. **Malware/viruses** – No person, including the Users, shall be permitted to use the School Assets or Personal Electronic Devices to transmit, download or store any virus, corrupted data or other harmful or destructive files that could damage or disrupts the performance of the School Assets; and

3.2.12. **Hacking –** No person, including the Users, shall hack or attempt to hack into the School Assets or any Personal Electronic Devices; access or attempt to access any information stored on the School Assets and/or Personal Electronic Devices, to which such person is not allowed access; or to manipulate the settings of same to, for instance, get around fire-walls etc.

3.3. **Content Filtering on School Assets**

3.3.1. As part of the Schools' continuing effort to protect its Users from the potentially harmful aspects of the Internet, whilst allowing them full access to the benefits that the Internet offers, state of the art security software ("the Software") has been installed on the School Assets.

3.3.2. The Software has been designed and implemented to monitor the websites that are accessed using the School's IT Infrastructure by all Users on an individual basis. The Software also monitors the exposure of the network to mailware, spyware, adware and virus intrusion. It has been designed to protect the system, network and servers as far as possible and thus will continually scan all directories, work that is produced on the computer and or saved on the computers, as well as any external media that are introduced to any part of the system by any person for material considered prohibited by this Policy.

3.3.3. Users are prohibited from circumventing or attempting to circumvent the Software.

3.3.4. Teachers may from time to time recommend and use public websites over which they have no control but that are, to the best of their knowledge, legitimate and safe.

3.3.5. It is recorded and accepted that whilst the School will make every effort to supervise User-usage of the School Assets, and the employment of the Software and fire-walls, usage of the School Assets may result in exposure to content that is inappropriate for school-aged minors. As a result of this, Users are required to take responsibility for their use of the School Assets and to avoid inappropriate content in so far as possible, and to report same to a member of staff.

3.4. **Monitoring of Activities on the School Assets: No Expectation of Privacy**

3.4.1. Users shall have **no expectation of privacy** in respect of their usage of the School Assets, including all information stored thereon.

3.4.2. It is recorded and accepted that all activity that takes place using School Assets is monitored and recorded. This includes, but is not limited to; email usage, web pages visited as well as all search queries used on sites such as Google and Wikipedia.

3.4.3. These recordings may be made available to the School's management upon request, to be examined and used as management, in its sole discretion, deems necessary (for example, to protect the health, safety, discipline or security of any person whether at the School or not).

3.4.4. Recordings and information located on the School Assets may also be used in disciplinary actions.

3.5. **Use of Personal Electronic Devices**

3.5.1. The School **does not allow** primary school Pupils to bring Personal Electronic Devices to School unless given express permission by their Parents **and** a teacher at the School.

3.5.2. The School **allows** high-school Pupils to bring Personal Electronic Devices to School (at their own risk) but these Personal Electronic Devices must not be removed from a Pupil's school bag during class-time, unless given specific permission by their Parents **and** the relevant member of staff at the School. If Personal Electronic Devices are found outside of bags during class time then the specific School Rules relating to same will apply.

3.5.3. The School may, from time to time, implement rules in terms of which use of and access to Personal Electronic Devices is regulated more or less heavily.

3.5.4. The School reserves the right to confiscate and examine the Personal Electronic Device of any User, including any audio or video recording stored on such device, where there is a reasonable suspicion by any member of staff or any administrator or representative of the School that such User is in breach of any provision of this Policy, any other School Policy or any other School Rule.

3.6. **The Right to Privacy**

3.6.1. The School respects the privacy of all Users, and expects those who use School Assets and Personal Electronic Devices to do so too when utilizing same.

3.6.2. In amplification of the above, unless given explicit permission by a member of staff or other representative of the School, no User may at any time take any picture, voice or video recording during any lesson or classroom activity.

3.6.3. Pupils, staff, Parents and third parties must not take pictures, voice or video recordings during break time or after-school activities, including during sporting events, music concerts or theatrical performances, unless given authorization in writing, and nor may they disseminate same. If authorisation is granted it may, however, be withdrawn at any time by any member of staff, in his or her sole discretion. Where any person is instructed by a member of staff to stop taking pictures, voice or video recordings in terms of this clause, they must cease to do so immediately.

3.7. **Consents**

3.7.1. The User hereby confirms that he/she consents, as contemplated under section 5 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, to the SABJE and/or the School intercepting and monitoring the content of any internet usage, email messages or any other direct or indirect communication sent or received on SABJE's or the School's computer facilities or infrastructure in order to monitor and ensure compliance with this Policy.

3.7.2. The User also confirms that he understands that the SABJE and/or the School may operate security software that monitors all computer usage and scans personal directories or work that he may produce or save on the SABJE and or the Schools computer facilities in order to ensure adherence to this Policy.

4. Disclaimer

4.1. The School and/or the SABJE accept no responsibility for Personal Electronic Devices. The responsibility to keep Personal Electronic Devices secure rests with the individual owner and the School and/or the SABJE will not be liable for any loss or damage to such Personal Electronic Device.

4.2. All access to and use of the School Assets and Personal Electronic Devices is at the sole risk of the User. The School and/or the SABJE makes no guarantees that the content available via the Network is free from errors or that the Network itself will be uninterrupted or error free.

4.3. Neither the School, nor any of its employees, other members of staff or governing bodies, shall be liable for any loss, damage or inconvenience of whatsoever nature arising directly or indirectly from:

4.3.1. the access or use by any person of the School Assets or Personal Electronic Devices;

4.3.2. the inability to use or access the Network;

4.3.3. the use by any person of any Personal Electronic Device;

4.3.4. any content existing on any Personal Electronic Device, or exposure of any person to content existing on any Personal Electronic Device;

4.3.5. the loss or theft of any Personal Electronic Device.

5. Disciplinary proceedings

5.1. Should any User be found to be in violation of this Policy, such User shall have their right to access the School's Assets temporarily or permanently suspended.

5.2. Should any person regularly breach this Policy they shall further be considered to have participated in Serious Misconduct and will be subject to disciplinary procedures as set out in the Code of Conduct.

5.3. In addition to the actions taken under the Code of Conduct Learners may also:

5.3.1. have their Personal Electronic Device confiscated for a period determined by the School in its sole discretion; and/or

5.3.2. be temporarily or permanently prohibited from bringing any Personal Electronic Device onto the School.

.

By signing this Policy, you indicate your understanding and agreement with it.

Signed on this _____ day of _____ 20_____

_____

Pupil's Signature

Pupil's Name: _____

_____

Parent's Signature

Parent's Name: _____

(By signing as a Parent you confirm that you have adequately explained this Policy to your child and that you will do everything in your power to ensure that they adhere to same and that you too will adhere to same.)