SPRINGS BOYS' HIGH SCHOOL

TECHNOLOGY POLICY

INTRODUCTION

Information Communication Technology (ICT) is utilized by Springs Boys' High School to enhance the learning process and to prepare our learners to embrace the challenges that the advance in technology brings. The processes and procedures regarding the use of all electronic Communication Devices (ECDs) used at Springs Boys' High School (including mobile phones) fall under the ambit of this policy.

Tablets, Smart phones, Laptops or any other device that has the capability to log onto the Internet or Wi-Fi service of the school would be categorized as ECDs

Directed use

The use of ICT will be based on the prescribed curriculum; furthermore the usage should be planned and directed towards the growth of both the learners and staff of Springs Boys' High school with the purpose of broadening their knowledge and skills base in order to achieve academic excellence.

Use of Technology: Terms and Conditions

1. **Personal information and user safety:**
   - Users will not post personal information about themselves or others. Personal information includes, but is not limited to the following: name, address, profiles, telephone, date of birth, pictures, etc.
   - Users will not arrange for meetings with anyone they have met online without the knowledge of the school and permission of a parent/guardian.
   - Users will promptly disclose to their educator or administrator any message they receive that is inappropriate or makes them feel uncomfortable.
   - Users will not harass another person or engage in personal attacks, including those prejudicial or discriminatory in nature following the guidelines of Springs Boys' High code of conduct.
   - All reasonable precautions must be taken to prevent others from gaining access to their account(s). All users are responsible for their individual account(s).
   - If a learner suspects a possible security issue, the learner must immediately inform his/her register teacher.
   - Learners and educators will not divulge passwords, codes, telephone numbers, account numbers, grades, or other school documents to unauthorized persons.
   - Deliberately posing as a user other than yourself is prohibited.

2. **Respect for Privacy**

   This includes but is not limited to:
   - Users will not forward or post a message that was sent to them privately without the consent of the person who sent it.
   - Users will not post private information about another person.
   - Users will not interfere with other users ECD work or files.

3. **Inappropriate Language**

   - Inappropriate language is seen as being in direct violation of the Springs Boys' High school code of conduct.
   - This includes, but is not limited to the use of obscene, profane, lewd, vulgar, offensive, inflammatory, threatening, or disrespectful language.

- Users will not participate in hate mail, harassment, discriminatory remarks, and other harmful or inappropriate behaviors.

4. Inappropriate Access to Material includes, but is not limited to:

- Users will not use school technology to access material that:
  - is profane or obscene (i.e. pornography),
  - advocates illegal or violent activities, or
  - advocates discrimination towards other individuals or groups
- If a user inadvertently accesses inappropriate material, he/she should immediately notify his/her teacher or administrator.
- Users will not deliberately attempt to override or circumvent firewalls or encourage others to do so.
- It is criminal offence, even for a child, to create, download, possess, distribute or display any child pornography.
- In South Africa the definition in The South African Films and Publications Act 65 of 1996 are used: "Child pornography includes any image, real or simulated, however created, depicting a person who is or who is shown as being under the age of 18 years, engaged in sexual conduct or a display of genitals which amounts to sexual exploitation, or participating in, or assisting another person to engage in sexual conduct which amounts to sexual exploitation or degradation of children."
- It is also a criminal offence, even for a child, to display or distribute any pornographic material, even to another child.

5. Technology Etiquette:

- Technology Etiquette includes, but is not limited to the following:
  - Be polite! Do not get abusive in your messages to others.
  - Exercise caution when using sarcasm and humour. Without face-to-face communications, a joke or statement may be misunderstood.
  - Show consideration and respect for others at all times.
  - Be respectful of the rights of other network users and do not violate their privacy.
  - Be aware of the intent and function of an individual or group before sending a message.
  - Deliberately posing as a user other than yourself is prohibited.
  - At the conclusion of a user's session that user will log off the system he/she is using.

6. Use of Equipment:

- Use caution when handling technology devices.
- Follow guidelines for proper usage of equipment.
- Do not use another person's computer resources without permission.
- Do not knowingly destroy any Electronic Communication Device (ECD) and/or technology equipment.

7. Security:

- Springs Boys' High School network and related technologies are the property of the school and therefore its storage systems is subject to inspection by school management. Learners, Educators and other staff should not have a privacy expectation in the contents of their personal files on the schools' intranet network or on ECD's used for school purposes.
- Springs Boys' High School reserves the right to monitor, or spot check, any Internet or electronic equipment devices (ECD) activities occurring on school equipment, accounts, and networks or on any ECD equipment utilized for educational purposes.
- Users will not attempt to gain unauthorized access to Springs Boys' High Schools' system(s), or to go beyond their authorized access.
- Users will not deliberately attempt to disrupt the performance of any computer system or destroy data via a virus or any other means.
- Users will not use the schools' system to engage in any illegal act.

- Vandalism of any kind will require restitution for costs associated with hardware, software and system restoration and could result in the cancellation of ECD privileges.

8. Plagiarism and Copyright:

- Users will respect the rights of all copyright owners, recognizing that infringement occurs when a person reproduces a work that is protected by a copyright. Students should check with teachers and support staff regarding relevant statutory laws.
- Users will not plagiarize; therefore, they should cite all quotes, references, and sources. Acknowledging the source of a copyrighted material does not substitute for obtaining reproduction rights.
- Users of ECD's at Springs Boys' High School will not install pirated software. All users should be aware that disseminating illegally obtained software is a crime punishable by law.

9. Respecting Resources:

- Users will use technology specifically for educational or career development activities.
- Users will not download large files or software programs without the authorization of the systems administrator. Software, particularly if it is offered as "free", comes with undetectable spyware and advertising that can disable a computer or an entire system.
- Users will not post chain letters or engage in "spamming" (sending unnecessary messages to a large number of people).
- Users will not use the network for personal and commercial purposes, such as, but not limited to, offering or purchasing goods and/or services for personal use.
- Users will not alter in any way the configuration of a computer or network without permission of authorized staff.
- Users will not intentionally waste resources, such as paper, ink cartridges, storage space, batteries, etc.
- Users acknowledge that information must be backed up and that it is the user's own responsibility to back up the data, if and when necessary.

10. Prohibited Use of Educational Technology:

- Users will not use any Springs Boys' High Schools' technology to play games that have been downloaded onto a technology device, or that are played on the Internet. Educator approved interactive tools, which are directly related to the curriculum, are permitted.
- Users will not use the Internet or other technology media to access chat rooms or any type of instant messaging.
- Users will have limited access to email, banking, and other personal accounts (not for running business or social accounts.
- Users will not access the Internet or other technology media for financial or commercial gain.Gambling, E-Bay shopping etc.)
- Users' activities, projects, or materials developed with technology and ECDs of Springs Boys' High School must reflect our educational standards and policies. This includes, but is not limited to web page designs, PowerPoint presentations, radio broadcasts, etc.
- Users will not impersonate other individuals real or fictional.
- Further personal causes such as political, religious or commercial views.
- Send/spread threatening or harassing messages.
- Send/spread sexually explicit or otherwise inappropriate material.
- Attempting to gain unauthorised access to computers, servers, Google Apps for Education accounts, voicemails or other ECD's.
- Purposely infecting the network or computers with spyware, malware or viruses.
- Gain access by using another's credentials.
- Use the Internet to access bandwidth grabbing programs unless authorized to do so.
- Violate copyright laws (anything from the Internet should be regarded as copyright protected).
- Download or upload any data or material not specifically related to your job/educational function.
- Users will not download, store, create or forward any information/data that is inflammatory, or defamatory to any race, creed, ethnicity, religion, sexual orientation or political beliefs of any individual or group.

- Users will not download any unauthorized software, file or program.
- Users will not download, store, create or forward any information regarding explosives or weapons unless such information is for a specific class assignment and the teacher has been consulted and granted permission.
- Harass others by repeated e-mails or IMs (Instant Messages) sent.
- Post real or altered images of others online.
- Post or solicit others to post nasty comments on a users' blog.
- Users will not engage in Cyber Bullying. Following is the definition for Cyber Bullying as described by Wikipedia:-

  The term "cyber bullying" is attributed to anti-bullying activist Bill Belsey.[1]

  ### Legal definition

  Cyber Bullying is defined in legal glossaries as:

  - actions that use information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm another or others.
  - use of communication technologies for the intention of harming another person
  - use of internet service and mobile technologies such as web pages and discussion groups as well as instant messaging or SMS text messaging with the intention of harming another person.

  Examples of what constitutes cyberbullying include communications that seek to intimidate, control, manipulate, put down, falsely discredit, or humiliate the recipient. The actions are deliberate, repeated, and hostile behavior intended to harm another. Cyberbullying has been defined by The National Crime Prevention Council: "When the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person."[2][3]

  A cyberbully may be a person whom the target knows or an online stranger. A cyberbully may be anonymous and may solicit involvement of other people online who do not even know the target. This is known as a 'digital pile-on.'[4]

  ### Cyberbullying vs. cyberstalking

  Further information: Cyberstalking

  The practice of cyberbullying is not limited to children and, while the behavior is identified by the same definition when practiced by adults, the distinction in age groups sometimes refers to the abuse ascyberstalking or cyberharassment when perpetrated by adults toward adults. Common tactics used by cyberstalkers are performed in public forums, social media or online information sites and are intended to threaten a victim's earnings, employment, reputation, or safety. Behaviors may include encouraging others to harass the victim and trying to affect a victim's online participation. Many cyberstalkers try to damage the reputation of their victim and turn other people against them.

  Cyberstalking may include false accusations, monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information in order to harass. A repeated pattern of such actions and harassment against a target by an adult constitutes cyberstalking.[5] Cyberstalking often features linked patterns of online and offline behavior. There are consequences of law in offline stalking and online stalking, and cyber-stalkers can be put in jail.[6] Cyberstalking is a form of cyberbullying.[*citation needed*]

  ### Methods used

  Manuals to educate the public, teachers and parents summarize, "Cyberbullying is being cruel to others by sending or posting harmful material using a cell phone or the internet." Research, legislation and education in the field are ongoing. Basic definitions and guidelines to help recognize and cope with what is regarded as abuse of electronic communications have been identified.

- Cyberbullying involves repeated behavior with intent to harm and repeated nature
- Cyberbullying is perpetrated through Harassment, Cyberstalking, Denigration (sending or posting cruel rumors and falsehoods to damage reputation and friendships), Impersonation, Exclusion (intentionally and cruelly excluding someone from an online group)[7]

Cyberbullying can be as simple as continuing to send e-mail or text harassing someone who has said they want no further contact with the sender. It may also include public actions such as repeated threats, sexual remarks, pejorative labels (i.e., hate speech) or defamatory false accusations), ganging up on a victim by making the person the subject of ridicule in online forums, hacking into or vandalizing sites about a person, and posting false statements as fact aimed a discrediting or humiliating a targeted person. Cyberbullying could be limited to posting rumors about a person on the internet with the intention of bringing about hatred in others' minds or convincing others to dislike or participate in online denigration of a target. It may go to the extent of personally identifying victims of crime and publishing materials severely defaming or humiliating them.[8]

Cyberbullies may disclose victims' personal data (e.g. real name, home address, or workplace/schools) at websites or forums or may use impersonation, creating fake accounts, comments or sites posing as their target for the purpose of publishing material in their name that defames, discredits or ridicules them.

Some cyberbullies may also send threatening and harassing emails, instant messages or texts to the victims. Others post rumors or gossip and instigate others to dislike and gang up on the target.

11. Educators and Social Networking:

- Educators are held to a higher standard and educators should use caution with text and photos that they may display. Educators may not use their ECD equipment during class time for social networking or for any other purpose than education and teaching.

12. Mobile Phones:

While mobile phones are important and useful, the use and abuse of mobile phones poses safety risks and has social and ethical consequences. The school does not allow learners to have mobile phones in their possession when they are in school uniform, or at school for the following reasons:

- Learners are targets for criminals and attacks on learners most frequently occur when they have been using their expensive, latest model mobile phones.
- Theft inside of school of learners’ mobile phones is a persistent problem.
- Learners do not look after their mobile phones and carelessly misplace them and then claim that the phones were stolen.
- In examinations and tests mobile phones are used to cheat with, therefore they are not allowed at all.
- Mobile phones allow learners access to lewd, inappropriate material, pornography etc. which is then disseminated.
- Mobile phones are a distraction and learners play on their mobile phones during class time and education suffers.
- Personal material on mobile phones and material such as photographs therefore become available to undesirables when the phone is stolen.

13. Mobile phones at Springs Boys’ High School is contrary to the Technology policy and Code of Conduct:

- Mobile phones used during school time will be confiscated for a determined period of time and could be up to three (3) calendar months.
- Mobile phones must be turned off (not on silent!) and may not be visible when they are on the school premises and especially during formal school time.

- Mobile phones will be confiscated if any transgression of the school Code of Conduct, Technology policy, any other school policy or South African law is suspected to further investigate the matter.

14. Kids Place Application:

- **Description:**

  "Kids Place" is an Android application that allows the school to completely block the use of certain applications on an android device. The applications that are allowed can be chosen by the administration.

  Any learner who uses their tablet for anything besides prescribed school work during class time, can have their tablet confiscated and it will be treated as a "First Offence", which is described below. Any learner who removes any restrictions placed on their device, without the explicit permission of school management, will be punished in accordance to the "Offence Management" policy.

- **Offence Management:**

  ~ **First Offence:**
  ∴ Should a learner be found using their tablet for anything that is not related to schoolwork, the normal confiscation policy applies. The learner will have to pay a fine of R50 and the "Kids Place" app will be loaded.

  ~ **Second Offence:**
  ∴ Should a learner be found on a website that is not allowed, the normal confiscation policy applies. The learner will have to pay a fine of R 50 before their tablet is returned to them, and all internet access will be revoked.
  ∴ Should a learner be found to have removed or circumvented the "Kids Place" app restrictions, the learner will be liable for a fine of R100.

  ~ **Third Offence:**
  ∴ Should a learner be found to have removed or circumvented the "Kids Place" app restrictions, the learner will be liable to re-purchase every single text book for each of their subjects. Text book costs are between R81 and R150 per book.

  ~ **Note:**
  If a learner commits any of the above offences: (i) an entry will be made in his personal file; (ii) the parent/s will be notified in writing and be expected to sign an acknowledgement letter; (iii) the learner will also sign an acknowledgement letter and (iv) last mentioned will be filed in the learners personal file.

15. Personal Security and ECD's:

- Learners should not display and use ECDs in public when on their way home with public transport or while walking home.
- Learners should consider their own safety and walk to their homes in groups and preferably not alone. (This is a general rule). Parents however have the final responsibility for learners' safety outside of school and must take responsibility for the learners transport arrangements.
- Thefts of ECDs on the school property must be reported to the school and a criminal case will be opened with the SAPS.

16. Consent:

- When accepting the Technology policy you undertake to consent to and adhere to the schools rules and authority regarding Information Communication Technology and Electronic Communication Devices.

SPRINGS BOYS' HIGH SCHOOL

ESTO PER PETUA

TECHNOLOGY POLICY ACCEPTANCE

Date: ____

Learners Name: ______________________________________

Learners Signature: ___________________________________

Parents Name: _______________________________________

Parents Signature: ____________________________________