INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

NEC ASPERA TERRENT

ST ANDREW'S COLLEGE

Contents

1 INTRODUCTION
2 OBJECTIVES OF THE POLICY
3 BACKGROUND
4 APPLICABILITY
5 DEFINITIONS
6 SECTION 1: USE OF SCHOOL EQUIPMENT
- 6.1 HARDWARE AND SOFTWARE
- 6.2 VIRUS PROTECTION
- 6.3 SECURITY
- 6.4 DATA STORAGE AND TRANSPORT
- 6.5 INTERNET CONNECTIVITY
- 6.6 PRINTING
- 6.7 LOSS AND DAMAGE
- 6.8 COMPUTER REPAIRS

7 SECTION 2: PERSONAL MOBILE DEVICES
- 7.1 GENERAL
- 7.2 CLASSES
- 7.3 CAMPUS
- 7.4 HOUSES

8 SECTION 3: NORMS OF BEHAVIOUR for ELECTRONIC COMMUNICATION
- 8.1 INTRODUCTION
- 8.2 ETHICAL PRACTICE
- 8.3 THE CLASSROOM
- 8.4 LANGUAGE USE
- 8.5 PORNOGRAPHY
- 8.6 BULLYING AND HARASSMENT
- 8.7 PLAGIARISM
- 8.8 THE INTERNET
- 8.9 EMAIL
- 8.10 SOCIAL MEDIA

9 SECTION 4: CONSEQUENCES OF BREACH OF THIS POLICY
10 GOVERNANCE
11 REVIEW

1. INTRODUCTION

The Information and Communication Technologies (ICTs) available at St Andrew's College (SAC) are easily accessible to all members of the school community. Because the administrative staff, teaching staff and pupils are dependent on technology to do their work, it is imperative that there is consensus on how the equipment is to be used and what it is used for. Clear guidelines need to be given and a code of conduct established. Agreement to the conditions specified is a requirement for all who wish to make use of the technology available at the school.

2. OBJECTIVES OF THE POLICY

This policy sets out the rules for the use of electronic equipment and the expected conduct for electronic communication. These are in line with and supported by the school rules as laid out in the SAC Handbook. The purpose of this policy is to endorse these rules and to underline how they apply to ICT at St Andrew's College. This policy includes rules and regulations for:

- The use of computers and other equipment
- The use of cellphones/smart phones and tablets
- The use of the internet
- Electronic communication

3. BACKGROUND

The financial investment the school has made and continues to make in technology is enormous. This applies to the equipment, the consumables, the staff to maintain the equipment and the staff with skills to keep the school at the cutting edge of modern technology for educational institutions. Further, the phenomenal growth in digital technology and the rise of social media have revolutionised the way people communicate and share information. The educational benefits of using electronic technology are that lessons can be enhanced and minds can be challenged in an extraordinary way. Pupils have the opportunity to collaborate with each other in innovative and novel ways. However, technology can be very disruptive when used inappropriately.

4. APPLICABILITY

This policy applies to anyone at SAC who uses the SDP network.
This policy deals with:

SECTION 1: The rules applying to the use of school equipment.
SECTION 2: The rules regarding the use of personal electronic devices.
SECTION 3: The norms of behaviour required for electronic communication using any electronic device.
SECTION 4: The consequences of disregarding the conditions laid down in this policy.

This policy is to be read in conjunction with the policies and principles that form part of the ethos and code of conduct of the schools and are governed by the schools' rules and regulations.

Applicable legislation includes but is not limited to:

1 The Constitution of South Africa:
2 The Films and Publication Act 65 of 1996
3 The Children's Act 38 of 2005
4 Criminal Law (Sexual offences and related matters). Amendment Act 32 of 2007
5 Protection from Harassment Act 17 of 2011
6 The Protection of Personal Information Act 4 of 2013
7 The Electronic Communication and Transactions Act 25 of 2002

5. DEFINITIONS

Authority/authorities	The person(s) to whom the Head has delegated authority to act on his behalf.
Bullying	Behaviour that can be construed to be systematic, uninvited, repeated and the intentional abuse of another person over a period of time.
Crack/cracking	The modification of software to remove or disable features such as copy protection. A crack refers to the means to achieve software cracking.
Cyberbullying	The use of electronic devices to deliberately upset or harm someone else.
St Andrew's College	St Andrew's College, Somerset Street, Grahamstown
Electronic communication	Any text, voice, sound or image message sent over an electronic communication network which is stored in the network.
Electronic device	Any device that can connect to the SDP network
Email	A message sent electronically from one computer to another or others via a network.
Equipment	All items needed and used that fall under the auspices of the ICT Department. This includes but is not limited to computers, speakers, recording devices, switches, cabling, and wireless access points.
Hack/hacking	Unauthorised entry into a computer system in order to steal, change or destroy information.
Hardware	The machines, wiring and other physical components of the SDP network.
Headmaster	The Headmaster of St Andrew's College.
Internet	The global computer network providing a variety of information and communication facilities.
MD	An abbreviation for personal mobile device (see below).
Mobile Devices Also Mobile Electronic Devices/ mobile personal device(s)	Cell phones, smart phones and tablets.
Pornography	Any content of a sexual nature that is illegal and/or that is deemed to be inappropriate by the school authorities.
Pupils	Boys who are registered as pupils at St Andrew's College.
School	St Andrew's College
SDP Network	The computer data network to which DSG, St Andrew's College and St Andrew's Prep School are connected.
Selfie	A photograph taken by the person of himself using a cellphone/smartphone/tablet and sharing it electronically.
Sexting	Sending, receiving or retaining sexually explicit text messages, pictures or videos digital media technology, with the volition of the person depicted.
Social Media	Any form of online publication or presence that allows users to engage in multi-directional conversations in or around the content on the website. Social media includes, but is not limited to Facebook, Ning, Twitter, YouTube, MXit, blogs, wikis, social bookmarking, document sharing and email.
Software	Programmes and other operating information used by a computer.
Virus	A piece of code introduced secretly into a computer system in order to damage, collect or destroy data.

6. SECTION 1: USE OF SCHOOL EQUIPMENT

All computers and devices connected to the network automatically fall under and are bound by the management practices of the ICT Department.

The rules and conditions of this policy are not meant to be restrictive. They serve to protect users of the SDP network and the network itself.

6.1 HARDWARE AND SOFTWARE

a. The school computers are a shared resource. As such, any form of tampering with hardware (computers, UPS, cabling, switches, data projectors, etc.) and software will be construed as vandalism.

b. No user may change any settings on a computer. This includes IP addresses, proxy server settings, DNS settings and domain settings and applies to all equipment (mouse, speakers, keyboards, printers, cameras, readers, etc.).

c. Devices or cables of devices attached to the network may not be changed.

d. No user may install any software (including screensavers, games, etc.) onto any school computer. All hardware and software installations have to be approved by the Head: ICT.

e. No copyrighted software – videos or music – may be downloaded from the Internet and placed on the computers' hard drive or the network drives. Commercial software is copyrighted and each purchaser must abide by the licencing agreement published with the software.

f. A 3G card may not be installed while a computer is connected to the network.

g. Software that the user has developed may be stored in the user's home folder, with the permission of the ICT department, provided that it falls into the category of academic software

h. No games may be stored (Windows games included) on any school computer or the network.

i. Pupils may connect one personal device to the network at no cost. Additional devices will be charged per term at a fee to be determined from time to time.

6.2 VIRUS PROTECTION

a. All personal computers must have virus protection before being connected to the network. The virus protection must be current and updated at least weekly. If so requested, the ICT Department will load an antivirus programme.

b. Searching for or downloading dangerous software is not permitted. This includes but is not limited to virus-, hacking- or spying software.

c. The ICT Department reserves the right to inspect any and all storage spaces for virus-infected files and unwanted files.

6.3 SECURITY

a. Users may not log onto the network using the credentials of any other user.

b. Users may not supply their login credentials to any other user. Users are to change their passwords should they suspect that the password may have been compromised.

c. Users will be held responsible for all activities performed with their network credentials.

d. Attempting to break into either the school's computer system or an off-campus computer system will be considered to be serious misconduct.

e. Attempting to obtain another person's password or using another person's password or interfering in any way with another person's data will be considered to be serious misconduct.

f. Impersonating another person by using a computer logged in as that user (described colloquially as 'raping') will be considered to be serious misconduct.

6.4 DATA STORAGE AND TRANSPORT

a. Users must store all data on their personal home drives or in a shared public folder. No data is to be stored on local workstations.

b. Users may not change or attempt to change any directory or folder settings such as ownership, security rights, share rights or any other settings.

c. Large attachments that are emailed will not be relayed.

6.5 INTERNET CONNECTIVITY

a. The school provides access to the internet through a login to the SDP data network.
b. Bandwidth is always at a premium. Users are urged to be considerate and limit the size of downloads.
c. Access to the network from Houses is restricted during school hours.
d. Access to internet sites and internet content is filtered by the school's firewall. The specific categories and rules of filtering are reviewed by the school from time to time.
e. Users may not bypass or attempt to bypass the school's firewall in any form or by any means.
f. All internet activities are logged, monitored and archived by the ICT Department.

6.6 PRINTING

a. Printing facilities are provided for pupils in designated areas around the school campus.
b. Access to printers is via login to the SDP data network.
c. All printing activities are logged, monitored and archived by the ICT Department.
d. Users should attempt to minimize printing by only printing documents that are absolutely necessary.

6.7 LOSS AND DAMAGE

a. Any device connecting to the SDP network is used entirely at the risk of the owner of the device. The school will not accept responsibility or liability for anything that may happen to any device while connected to the school's network or servers.
b. The school does not accept responsibility for users' data loss.
c. Whilst every effort will be made to ensure that boys cannot access inappropriate information, the school cannot be held liable if a boy takes it upon himself to access such material. Such instances, if identified, will be regarded as serious misconduct.
d. The school advises that all mobile devices used on campus should be pin-protected and/or have security enabled to ensure data protection and to prevent unauthorised use. The ICT Department can advise.

6.8 COMPUTER REPAIRS

The ICT Department is responsible for maintaining school ICT equipment and services that enable staff and pupils to perform their duties. Computer repairs and are thus carried out in a strict order of priority:

- Critical operations and core business
- Non-critical operations and core business
- Staff and pupils' personal computers and devices

7. SECTION 2: PERSONAL MOBILE DEVICES

(In this section, these will be referred to collectively as MDs. This abbreviation refers to cell phones, smartphones and tablets).
The ***Privacy to Personal Information*** law applies. Any personal information that can identify a person cannot be shared on any public forum without the permission of the person.

7.1 GENERAL

a. Pupils are permitted to have mobile devices (MDs) at school.
b. If a pupil has an MD with her at times when it may not be used, it must be on silent or turned off. If an MD rings during these times, the MD may be confiscated for a period to be determined by the person in charge.
c. The school accepts no responsibility for any loss of or damage to MDs, whether on campus or elsewhere. It is strongly advised that they store their MDs in a safe place when not in use.
d. The school's Search and Seizure Policy applies to pupils' MDs.

7.2 CLASSES

a. It is the prerogative of the teacher of the specific class to decide if, when and how MDs will be used during that class.

b. Before tests or exams, pupils must hand in all MDs to the invigilators. MDs must be clearly marked with the owner's name. MDs can be collected after the test/exam papers have been handed in at the end of the exam.

c. Any pupil found in possession of an MD during a test or exam, even if inadvertently, will be found guilty of cheating.

7.3 CAMPUS

a. Pupils may not have cell phones on the campus between 07:30 and 15:00 on weekdays (07:30 and 13:05 on Wednesdays).

b. MDs may not be used during gatherings. This includes but is not limited to:

- □ meals
- □ chapel services
- □ assembly
- □ prize-giving
- □ an outing with the school
- □ any formal gathering

7.4 HOUSES

Grade 8s and Grade 9s are required to hand their MDs to the Housemaster at bedtime.
These will be returned the next day.

8. SECTION 3: NORMS OF BEHAVIOUR for ELECTRONIC COMMUNICATION

8.1 INTRODUCTION

Pupils in South Africa and across the world are becoming more and more engaged in social net working, blogging, wikis and many other forms of cyber-communication. Schools are now being challenged with regard to how cell phones/ smart phones/ tablets can be used in constructive and educative ways, especially in classrooms and as part of the learning experience at school. At the same time, schools have to manage the use of these devices to avoid the possible risks that can be incurred from careless or malicious use.

The policies and guidelines given in this section serve both to encourage and extend the use of electronic devices in constructive and educative ways as well as to limit and contain the possibilities of destructive or counter-productive instances.

8.2 ETHICAL PRACTICE

All members of the SAC community are expected to honour the school's values and practices. In doing so, they will not:

- bring the school into disrepute
- post any material on a website without the permission of the person or entity involved
- create a persona or digital ID on any social media site (eg., Facebook, Twitter) which represents or pretends to represent the school without the approval of the Head.

8.3 THE CLASSROOM

a. When teachers use or allow the use of the internet and/or social media for schoolwork, either in the classroom or as required work outside the classroom, participation in such online media is an extension of their classrooms in terms of what is permitted/acceptable online.

b. Photographs may not be taken or videos or recordings made in a class without the permission of the teacher concerned.

8.4 LANGUAGE USE

a. Messages posted publicly must not include any personal attacks (colloquially known as 'flaming')

b. Messages should follow the rules of appropriate public language.

c. Any text transmitted to a public environment may not contain any language or content that the author would not be willing to share from the podium at a school meeting.

8.5 PORNOGRAPHY

Both the Film and Publications Act and the Sexual Offences Act make it an offence for a person under the age of 18 to:

- View pornography
- Be in possession of pornography
- Download pornography from the internet
- Trade in pornography
- Enter a licenced premises where pornography is legally sold
- Expose another person under the age of 18 to pornography

8.5.1 Child pornography

According to the South African law, child pornography is deemed to be any naked image showing genitalia of a person under the age of 18.

8.5.2 Pornography at school

a. Possession or distribution of pornography at school is considered to be serious misconduct. According to the SAC Handbook, viewing and/or circulating any material deemed by those in authority to be pornographic is a serious offence.

b. As well as the above, activities that would be considered to be pornography include, but are not limited to: sexting, distributing naked 'selfies', distributing photographs/videos of a naked friend, distributing photos/videos of anyone involved in sexual activities.

8.6 BULLYING AND HARASSMENT

The following behaviour is unacceptable at all times:

a. Attacking SAC, the staff, the pupils or other people on any digital communication forum

b. Cyber-bullying. According to the school's bullying policy, bullying includes but is not limited to:
   - behaviour that can be construed to be the systematic, uninvited, repeated and intentional abuse of another person over a period of time
   - harming another person (hurting or embarrassing another person)
   - repeated threatening behaviour which is intended to frighten another person
   - using electronic technology; for example, text messages or emails, rumours sent by email or posted on social networking sites, embarrassing pictures, videos, websites or fake profiles.

c. Insulting others

d. Using racist or sexist language

e. Passing derogatory or offensive comments

8.7 PLAGIARISM

Plagiarism includes but is not limited to:

- Downloading information from the internet and portraying it as personal work
- Copying another pupil's work
- Presenting another person's ideas as being original

All information downloaded from the internet must be referenced with the name of the site, the title and author of the article (if given) and the date accessed.

8.8 THE INTERNET

a. Users may not:

- access material that is labelled as 'not intended for minors', even if they have turned 18.
- download, make public or intentionally view any material that is pornographic, abusive or age-restricted.
- disseminate the addresses of any material that falls into one of the above categories.

b. All internet activities are logged, monitored and archived by the IT Department.

8.9 EMAIL

SAC regards emails to be the same as paper messages. Therefore any written communication should obey the correct rules of grammar, capitalisation and punctuation.

a. Users must accept the privacy of email messages; mail may not be read by another person and care must be exercised when forwarding messages to ensure that privacy is not compromised.

b. Electronic mail may not be misused. The following are considered to be misuse:
   - unacceptable language
   - offensive messages
   - mass mail
   - hate mail
   - junk mail
   - sending or distributing games
   - personal graphic images
   - chain letters
   - hoaxes
   - anonymous mail
   - age- restricted content
   - distribution of viruses, hacks or cracks

c. No email or attachment from an unknown source should be opened. These should be deleted.

d. According to the Search and Seizure Policy, the school authorities are entitled to intercept and monitor email messages, laptop content or other communication sent or received in order to monitor and ensure compliance with these terms of use.

8.10 SOCIAL MEDIA

a. Where pupils are engaged in online activities, they must remember that social media are by their very nature public domains and appropriate care needs to be taken when using them.

b. Where girls can be identified with the school and are inappropriately engaged, the school can intervene to prevent reputational damage to the school and/or to the individuals involved. Such abuse of the media could result in disciplinary action.

c. The rules of the school and the code of conduct should be adhered to when communicating online.

d. Users may not download, make public or intentionally view any material that is pornographic (See 8.2 item c. above).

e. It is acceptable to disagree with someone’s comments, but this must be done in a respectful way. Any criticism must be constructive and not harmful.

f. According to the Search and Seizure policy, the school authorities are entitled to seize any MD or computer and monitor any activity of the user.

9 SECTION 4: CONSEQUENCES OF BREACH OF THIS POLICY

The violation of school rules concerning the use of the network will result in the same disciplinary actions as would result from similar violations in other areas of SAC life.

Any breach of this policy will be dealt with according to the Discipline policy of the school.

10. GOVERNANCE

Good governance requires that all documentation pertaining to notes kept by Reporting Officers, Investigations and Disciplinary Hearings and Appeals are confidential and, as such, kept in a secure environment. All findings must be documented and kept in a secure environment.

11. REVIEW

This policy will be reviewed every three years by the Director of ICT at SAC, the Headmaster and any persons nominated by the Headmaster