Prestige College Schools

Information & Communication Technology (ICT) Use Policy

(updated on 4 March 2019)

1.INTRODUCTION

This policy reflects the Prestige College Schools' values and ideals in relation to teaching and learning of the South African National School Curriculum using Information Communication Technology as a platform. It is recognized that ICT devices/equipment bring great benefits to teaching and learning programmes, and the Schools place a high priority on Intranet facilities and ICT devices and equipment which will facilitate learning outcomes. However, in the presence of an ICT learning environment cognizance must also be taken of its ability to facilitate anti-social, inappropriate, and even illegal, material and activities. This policy reflects the Schools' responsibility to maximize the benefits of these technologies, whilst at the same time to minimize and manage the risks.

The Schools thus acknowledge the need to have in place a rigorous and effective ICT Policy, which provides adequate guidance on acceptable usage and prohibitive actions including adequate cyber safety practices. This ICT Policy is designed to facilitate responsible, respectable and lawful use of the schools' ICT framework for all Users which is aligned to the Schools' Code of Conduct and South African Legislation regulating ICT including the Electronic Communications and Transmissions Policy.

2.DEFINITIONS

Important terms used in this document:

'ICT' in this document refers to the term 'Information and Communication Technology;

'Cyber safety' refers to the safe and responsible use of the Intranet and ICT equipment/devices, including mobile phones;

'Schools' means **PRESTIGE COLLEGE SCHOOLS;**

'School ICT' refers to the school's computer network, Intranet access facilities, computers, and other school ICT equipment/devices as outlined below;

'ICT equipment/devices' used in this document, includes but is not limited to all types of computers, tablets, storage devices, cameras, mobile phones, gaming consoles or any other technologies that may come into use and are used in information, data, images, audio, applications and software storag;

"Users" means Learners, all Staff, Service Providers, Parents and Visitors to the School Premises.

3. CONSEQUENCES FOR VIOLATION OF COMPUTER USE POLICY AND RULES

- Unacceptable and/or unlawful use of the Schools' ICT systems and ICT devices/equipment constitute a breach of schools' rules and any User who violates this policy and rules may have their ICT privileges limited, suspended or revoked and may also face disciplinary procedures dependant on the severity of the infraction which shall be dealt with on a case-by-case basis. Any ICT equipment /device belonging to the User may accordingly be

confiscated.

- Certain violations may also result in referral to law enforcement and/or legal action. Enclosed herewith is a list of relevant legislation governing ICT law at schools. Transgressions hereof are punishable by law so adherence to this policy is vital.

4.ACCEPTABLE USE

- The Schools' ICT is provided for educational purposes only and must be regarded as a privilege and not a right and usage must be consistent with this policy, cyber safety and directly related to the educational objectives of the School.
- The Schools have the right to place reasonable restrictions on the material you access or post, the training you need to have before you are allowed to use the system, and enforce all rules set forth in the School Code.
- Under the following activities which are authorized by an Educator or the School:
    - Researching information relating to a school assignment;
    - Gathering specific information about subjects/topics;
    - Collaborative learning projects;
    - Emailing a Teacher or Learner for assistance with school related work;
    - Other Teacher directed activities.

5.PROHIBITED USES

Prohibited uses of School ICT that are expressly prohibited include, but are not limited to, the following:

- Accessing, submitting, posting, publishing, distributing or intentionally accessing forwarding, downloading, scanning or displaying defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal materials without redeeming educational value or deemed harmful to minors, which is defined as any picture, image, graphic image file, or other visual depiction that:
    - taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
    - depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition; or
    - taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors

- Using the Schools' ICT for any illegal activity or in violation of any School policy and rules, including bullying or harassing behaviour toward Learners or other persons, including:
    - Attempting to harm, modify or destroy data of another User.
    - Attempting to gain unauthorized access to programs or computer equipment, including attempts to override any firewalls established on the Schools' ICT network.
    - Using the Schools' ICT in a manner that would violate any South African legislation and

subjects the User and or the Schools to any civil or criminal action. This includes, but is not limited to, the transmission of threatening material, the spreading of computer viruses, participating in software piracy, using the Schools ICT for purposes of gambling, or arranging for the sale or purchase of drugs or alcohol.

- Sending "chain letters" or "broadcast" messages to lists or individuals or subscribing to "list serves" or "newsgroups" without prior permission.
- Computer games are (in general) not part of the school curriculum and should not be played in class or in any area of the school unless a specific classroom task using a game format is set as a valid, assessable activity.

- Using the Schools' ICT for **commercial purposes** to offer, provide, or purchase products or services.

- **Violating Copyrights,** through copying, downloading or sharing any type of copyrighted materials (including music or films) without the owner's permission; copying or downloading Software or without the express authorization of the Schools, recognising that unnauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties.

- **Plagiarism** or representing as one's work any material obtained through the internet or other data sources, including the on the Schools' ICT system, which is a reportable and criminal violation.

- **Misuse of Passwords/Unauthorized Access** by sharing passwords, using other Users' passwords, and accessing or using other users' accounts.

- **Bringing any inappropriate material to school** in any form, including electronic form. Teachers may check learners' storage devicies and all ICT equipment/devices at any time whether as part of a regular survey or upon a reasonable suspicion that the Learner has violated this policy in any manner and remove any offending material and report the incident in accordance with the Schools rules.

- **The malicious use, disruption or harm to the School ICT** or any other users' devices, including but not limited to hacking activities and creation/ uploading of computer viruses.

- **Language use** that includes inappropriate, obscene, inflamatory, threaterning, defamatory, discriminatory or harassing content.

- **Intercepting and/or changing or deleting** any electronically based messages intended for someone else.

- **Posting or personal, private or protected information** relating to oneself, the

school or other users/learners/staff.

- Any unauthorised recording regardless of the device used, of school activities; classroom proceedings; videos, photos or images of staff; learners or visitors to the school.

6.PUBLISHING ON-LINE CONTENT

No member of staff, learner or parent shall publish any images, videos, blogs, voice notes or documents that refer to any of our schools and which results in the school being regarded in a negative light. The school will act decisively against anyone found guilty of bringing the school into disrepute through any such actions of publishing inappropriate content and negative comments on the internet. Those who are dissatisfied with their experience of the school in question shall raise their issues with the School's Leadership Team and if this does not lead to a resolution of the problem, their request shall be referred to the Director Operations.

7.E-MAIL

- Users may only use approved e-mail accounts on the school system.
- Learners must immediately tell a teacher if they receive offensive e-mail.
- Staff to Learner e-mail communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

8.PUBLISHING PUPIL'S IMAGES AND WORK

All school marketing and recognition of achievements activities includes photographs of learners in action on the sports field, in cultural acvitities or in academic pursuits. It is assumed that unless expressly prohibited by the parents of the learners, that the schools are permitted to use the photos of learners in a responsible manner and wherever possible preferably in groups. The identification of learners in photographs will be carefully considered and such will only be done if it is to the benefit of the learners in terms of being recognised for his/her achievements. **Any parent/guardian who expressly prohibits the schools to use photographs of learners under their care, must do so in writing to the Principal of the particular school.**

9. PRIVACY IS NOT GUARANTEED

The Schools will monitor all computer related activities of Users and may employ technology protection measures during any use of such computers by Users. These technology protection measures utilized will block or filter Internet access to any visual depictions that fall in the category of prohibited uses as in paragraph 5. It should be noted though that despite the schools' efforts to install protection software, complete privacy and protection cannot be guaranteed.

Although Prestige College Schools respect learner's right to privacy, we retain the right to monitor and intercept electronic communications in accordance with the Interception of

Communications and Provision of Communications related- Information Act of 2002. This includes the access of the phone by qualified technicians under supervision of the school and/or the police where it is deemed necessary for investigation purposes.

10. MOBILE PHONES

- The **Schools accept** that we're operating in a digital and mobile communications environment, in which the use of cellular or smart phones has become a vital component not only of day to day communication, but also plays a key role in securing the safety of minors. The Schools do however require the responsible use of these mobile phone devices at all times, in keeping with the Acceptable and Prohibited Uses as contained in paragraphs 4 and 5. The following key regulations apply to cellular or smart phones:
- **Primary School learners** (up to grade 7) will not be allowed to use a mobile phone anywhere and at any time on the premises of the school without express authorisation from a teacher. It is advisable that learners in the primary school do not carry mobile phones as the school takes no responsbibility for breakage or theft. Any learner found using a mobile phone will have the phone confiscated and this phone will only be released to a parent on proof of payment of a R 300 phone release fine, into the school's bank account.
- **Secondary School learners will be allowed** to carry mobile phones, provided they abide to the conditions stated. Failure to do so will also see the phones confiscated and a release fine of R 300 be applied. The school takes no responsibility whatsoever for any damage or loss related to mobile devices brought onto the premises or while the learner travels to and from the school. Unless approved by the specific class teacher to be switched on for educational purposes, all phones will remain switched off during the academic classes.
- **During formal tests and exams** no phones are allowed in the exam venue. Learners shall make the necessary arrangements for the safekeeping of phones and it preferred that on such days phones remain at home if at all possible. The school will again not accept any responsibility for loss, theft or damage.
- **Any form or harassment, bullying** in whatever form, defamatory or discriminatory communication will lead to the immediate confiscation of the device(s) used and where necessary the actions would be referred to the local South African Police Services for handling in respect to common law.
- **The Schools regard the abuse of mobile phones and social media as a heinous transgression** and will apply a harsh no tolerance approach to correction if any learner, staff member or visitor to the school is found guilty of such behaviour.

11. INDEMNIFICATION

The Learners Parent/ Guardian indemnifies and holds the Schools and or its Board harmless from any claims, including attorney's fees, resulting from the User's activities while utilizing the Schools ICT and any ICT device/equipment.

12. POLICY REVIEW

Because of the rapid changes in the development of ICT regulations, the School Board shall conduct an annual review of this policy.

13. ADDENDUMS - IMPORTANT STATUTES WHICH ARE APPLICABLE TO LEARNERS USE OF SCHOOL ICT INCLUDE:

The Copyright Act, 1978 (Act No. 98 of 1978)

Learners may copy or otherwise deal with copyright material for the purpose of study or education. However, generally only the author of original material has the right to reproduce, copy, publish, perform, communicate to the public and make an adaptation of the copyright material.

The Promotion of Equality and Prevention of Unfair Discrimination Act 2000 (4 of 2000) prohibits the following:

- dissemination and publication of information that unfairly discriminates on the basis of sex, marital status or pregnancy, family responsibility or family status, sexual orientation, race, religious or political conviction, impairment or age in education
- Hate speech and harassment in workplace and educational institutions.

The Electronic Communications and Transactions Act 2002 (25 of 2002)

- To provide for the facilitation and regulation of electronic communications and transactions;
- to prevent abuse of information systems.
- Cyber-crime is defined under section 86 as follows:

  Unauthorized access to, interception of or interference with data. 86. (1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1993), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence. (2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence. (3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possess any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilize such item to contravene this section, is guilty of an offence. (4) A person who utilizes any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence. (5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of

service to legitimate users is guilty of an offence.

Protection of Harassment Act 2010 (17 0f 2010)

- Since the Bill of Rights in the Constitution of the Republic of South Africa, 1996, enshrines the rights of all people in the Republic of South Africa, including the right to equality, the right to privacy, the right to dignity, the right to freedom and security of the person, which incorporates the right to be free from all forms of violence from either public or private sources, and the rights of children to have their best interests considered to be of paramount importance;
- And in order to afford victims of harassment of an effective remedy against such behaviour; provide for easy access to the courts of law for protection.