PRESTIGE COLLEGE

ICT POLICY 2016

Parents will receive this contract to keep as their reference. On the application form the parents who applied will sign the APPLICATION FORM, acknowledging their understanding and agreement with the content of this policy.

1 INTRODUCTION

1.1 This policy reflects the Schools values and ideals in relation to teaching and learning of the South African National School Curriculum using Information Communication Technology as a platform.

1.2 It is recognized that ICT devices/equipment bring great benefits to teaching and learning programmes, and the School places a high priority on Intranet facilities and ICT devices / 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.

1.3 The School thus acknowledges 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.

1.4 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:

2.1 'ICT' in this document refers to the term 'Information and Communication Technology;
2.2 'Cyber safety' refers to the safe and responsible use of the Intranet and ICT equipment/devices, including mobile phones;
2.3 'School' means **PRESTIGE COLLEGE;**
2.4 'School ICT' refers to the school's computer network, Intranet access facilities, computers, and other school ICT equipment/devices as outlined in 2.5 below;
2.5 'ICT equipment/devices' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and

audio players/receivers (such as portable CD and DVD players),Gaming Consoles, and any other, similar, technologies as they come into use;

2.6 "Users" means Teachers, Learners and all other School staff members.

3 CONSEQUENCES FOR VIOLATION OF COMPUTER USE POLICY AND RULES

3.1 Unacceptable and/or unlawful use of the School ICT systems and ICT devices/equipment constitutes a breach of school 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 according be confiscated.

3.2 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

4.1 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.

4.2 The Schools has 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.

4.3 Under the following activities which are authorized by an Educator or the School

4.3.1 researching information relating to a school assignment;
4.3.2 gathering specific information about subjects/topics;
4.3.3 collaborative learning projects;
4.3.4 emailing a Teacher or Learner for assistance with school related work;
4.3.5 other Teacher directed activities.

5 PROHIBITED USES

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

5.1 Accessing Inappropriate Materials:

5.1.1 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;

5.1.2 Including visual depictions that are:

5.1.2.1 Obscene;

5.1.2.2 Child pornography;

5.1.2.3 Harmful to minors.

The term “harmful to minors” means 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

5.2 Illegal Activities:

5.2.1 Using the Schools ICT for any illegal activity or in violation of any School policy and rules, including bullying or harassing behavior toward Learners or other persons.

5.2.2 Attempting to harm, modify or destroy data of another User.

5.2.3 Attempting to gain unauthorized access to programs or computer equipment, including attempts to override any firewalls established on the Schools ICT network.

5.2.4 Using the School ICT in a manner that would violate any South African legislation and subjects the User and or the School 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.

5.2.5 Sending “chain letters” or “broadcast” messages to lists or individuals or subscribing to “list serves” or “newsgroups” without prior permission.

5.2.6 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.

5.3 Users may not use the School ICT for commercial purposes to offer, provide, or purchase products or services.

5.4 Violating Copyrights:

5.4.1 Copying, downloading or sharing any type of copyrighted materials (including music or films) without the owner's permission.

5.4.2 Copying or downloading Software or without the express authorization of the School.

5.4.3 Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties.

5.5 Plagiarism:

Representing as one's work any material obtained on the School ICT which is a reportable and criminal violation;

5.5.1 Misuse of Passwords/Unauthorized Access: Sharing passwords, using other Users' passwords, and accessing or using other users' accounts.

5.5.2 Learners are not permitted to bring inappropriate material to school in any form, including electronic form. Teachers may check learners USB thumb drives and all ICT equipment/devices 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 School rules.

5.6 Malicious Use/Vandalism: Any malicious use, disruption or harm to the School ICT including but not limited to hacking activities and creation/ uploading of computer viruses.

6 INAPPROPRIATE LANGUAGE

6.1 On any and all uses of the School ICT, whether in application to public or private messages or material posted on the portal, the User will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

6.2 Users shall not post information that could cause danger or disruption or engage in personal attacks, including prejudicial or discriminatory attacks which is based on religious preferences, ethnic and political views or gender and race bias.

6.3 Users shall not harass another User other person by a persistent action that distresses or annoys another User / other person and the User shall immediately stop when asked to do so or disciplinary procedures shall be procured.

7 SCHOOL ICT ETIQUETTE

Each User is expected to abide by generally accepted rules of etiquette, including the following:

7.1 Be polite!!!! Don't be abusive when addressing others including other Users.
7.2 Users shall not forge, intercept or interfere with electronic mail messages.
7.3 Use appropriate language. The use of obscene, lewd, profane, threatening or disrespectful language is prohibited.
7.4 Users shall not post personal contact information, including names, home, school or work addresses, telephone numbers, or photographs, about themselves or others.
7.5 Users shall respect the computer system's resource limits.
7.6 Users shall not post chain letters or download large files.
7.7 Users shall not use the computer system to disrupt others.
7.8 Users shall not read, modify or delete data owned by others.

8 E-MAIL

8.1 Users may only use approved e-mail accounts on the school system.
8.2 Learners must immediately tell a teacher if they receive offensive e-mail.
8.3 Learners must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
8.4 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.
8.5 Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

9 PUBLISHING PUPIL'S IMAGES AND WORK

9.1 Photographs that include Learners and their work will be selected carefully. The School will look to seek to use group photographs rather than individual children except where individual children achieved great heights in any school activity.

9.2 Learner's full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

9.3 The school obtained permission from parents through the parent contract with the school that photos of learners may be used on the school's social platforms where appropriate as part of a school activity.

10 PRIVACY IS NOT GUARANTEED

10.1 The School will monitor all computer related activities of Users and may employ technology protection measures during any use of such computers by Users.
10.2 The technology protection measures utilized will block or filter Internet access to any visual depictions that are: Obscene; Child pornography; or that is Harmful to minors.

11. MOBILE PHONES

11.1 Acceptable Use

11.1.1 The increased ownership of mobile phones requires that School Administrators, Teachers, Learners, and Parents take steps to ensure that mobile phones are used responsibly.

11.1.2 The School wishes to ensure that potential issues (such as mobile etiquette) can be clearly identified and addressed; ensuring the benefits that mobile phones provide (such as increased safety and security) can continue to be enjoyed by our Learners.

11.2 Personal safety and security.

11.2.1 The School accepts that Parents give their children mobile phones to protect them from everyday risks involving personal security and safety.

11.2.2 There is also ever-increasing concern about children travelling alone on public transport or commuting long distances to school. It is acknowledged that providing a child with a mobile phone gives Parents reassurance that they can speak with their child quickly, at any time.

11.3 Responsibility of Secondary learners

11.3.1 It is the responsibility of Learners who bring mobile phones onto School premises to adhere to the guidelines outlined in this policy.

11.3.2 The decision to provide a mobile phone to their children should be made by Parents or guardians.

11.3.3 Parents should be aware if their child takes a mobile phone onto school premises.

11.3.4 Mobile phones must normally be switched off during classroom lessons. Exceptions may be permitted in rare circumstances, should the Parent/guardian specifically request it. Such requests will be handled on a case-by-case basis, and should be directed to the Principal.

11.3.5 Parents are reminded that in cases of emergency, the School Office remains a vital and appropriate point of contact and can ensure your child is reached quickly, and assisted in any appropriate way. Parents are not allowed to phone their children during class time. Children will lose points if answering phones during class time.

11.4 Primary

11.4.1 Mobile phones must be kept in at the office or school bag during the school day.

11.4.2 Learners are not permitted to use their mobile phones at all during the day.

11.4.3 If a Learner needs to make a telephone call during the day they must ask permission from the class teacher and a school telephone will be used if deemed appropriate.

11.4.4 Any mobile phone being used during the day will be confiscated.

11.5 Theft or damage

11.5.1 Learners are required to mark their mobile phone clearly with their name.

11.5.2 Mobile phones which are found in the School and whose owner cannot be located should be handed to the office until proof of ownership established and consent forms signed by the Parent/ Guardian and Learner.

11.5.3 The School accepts no responsibility for replacing lost, stolen or damaged mobile phones. Their safety and security is wholly in the hands of the Learner.

11.5.4 The School accepts no responsibility for Learners who lose or have their mobile phones stolen while travelling to and from School.

11.5.5 It is strongly advised that Learners use passwords/pin numbers to ensure that unauthorized phone calls cannot be made on their phones (e.g. by other Learners, or if stolen). Learners must keep their password/pin numbers confidential. Mobile phone and/or passwords may not be shared**.**

11.6 Inappropriate conduct

11.6.1 Any Learner found using a mobile phone to gain advantage in exams or assessments will face disciplinary actions as sanctioned by the School. That would be considered as dishonesty which is an expellable offence.

11.6.2 Any Learner who uses vulgar, derogatory, or obscene language while using a mobile phone will face disciplinary actions as sanctioned by the School.

11.6.3 Learners with mobile phones may not engage in personal attacks, harass another person, or post private information about another person using SMS messages, taking/sending photos or objectionable images, and phone calls.

11.6.4 Learners using mobile phones to bully other Learners will face disciplinary actions as sanctioned by the School.

11.6.5 It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. As such, if action as sanctioned by the School is deemed ineffective, as with all such incidents, the School may consider it appropriate to involve the police.

12 CYBERBULLING

12.1 Cyberbullying is the use of ICT, particularly mobile phones and the internet/intranet, deliberately to upset someone else.

12.2 Cyberbullying may consist of threats, harassment, embarrassment, humiliation, defamation or impersonation. It may take the form of general insults or prejudice based bullying for example homophobic, sexist, racist or other forms of discrimination. It may include photographs or video clips taken by mobile telephone.

12.3 The School has a no tolerance policy in relation to all forms of bullying whether it be against Learners or Teachers and takes a very proactive stance in which any bullying of whatever nature will always be investigated thoroughly and dealt with in accordance with the Schools disciplinary procedures and the severity thereof will be taken into consideration when confiscating and or suspending the Learners ICT privileges and attendance at this School including police intervention and civil actions.

13 POLICY REVIEW

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

14 INDEMNIFICATION

The Learners Parent/ Guardian indemnifies and holds the School 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.

Learner Authorization:

I certify that I have read and that I understand the School ICT Policy. I agree to abide by all the terms and conditions stated in this policy. I understand that if I violate any terms or conditions set in this policy, my Intranet/Internet access privilege may be revoked and that I will be subject to disciplinary action. I also understand that violation of this policy may subject me to criminal and/or civil proceedings

Learners Name: (please print)_____

Learners Signature: _____

Date:_____

Parent /Guardian Authorization:

As Parent /Guardian of the above named Learner, I have read and discussed the School ICT Policy with my child. I understand that this access is designed for educational purposes. I understand that some materials accessed on the Intranet/Internet may be illegal, defamatory, inaccurate, or potentially offensive, and although the School has taken precautions to filter these materials, such exposure may still occur. I understand that if my child should commit any violation, his/her access privileges may be revoked and school disciplinary action will be taken including criminal /civil proceedings. I accept all financial and legal liabilities that may result from my child's unacceptable use of the Intranet/Internet. In addition, I accept full responsibility for the supervision of my child, if and when he/she uses the Internet outside of a school setting.

Parent/Guardian Name (please print):

_____

Signature: _____
(Required)

Date: _____

ATTACHMENT

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 behavior; provide for easy access to the courts of law for protection.