INFORMATION TECHNOLOGY POLICY:

BLUE HILLS COLLEGE

Document Reference:	
Document Type:	Policy Document
Version:	2.1

DOCUMENT CONTROL

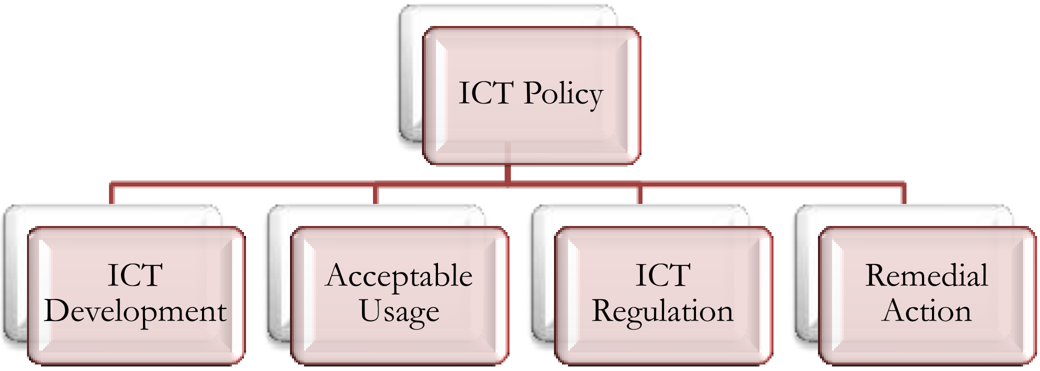
POLICY AIM:	To manage and control the use and access of electronic ICT, cellular technology and social media by students at **Blue Hills College**
APPLICABILITY:	All students and teachers of **Blue Hills College**

1. INTRODUCTION

Efficiency in the use of Information Communication Technology (ICT) is becoming an integral part of our modern-day society, from an early age on. Pupils need to be fluent in its use for learning, leisure and academic work. Therefore at **Blue Hills College** we believe that ICT deserves to be integrated with our learning curriculum.

ICT is becoming an efficient medium for finding and using information as part of the learning process. By utilising an effective ICT strategy we will encourage pupils to fully utilise the ICT resources to improve their quality of work and presentation skills across all subjects.

This ICT policy serves as a mechanism to constantly improve our teaching methods and presentation of the subject, thereby developing ICT skills across all year groups and subject areas in a safe and regulated environment. The **Blue Hills College** ICT pillars:

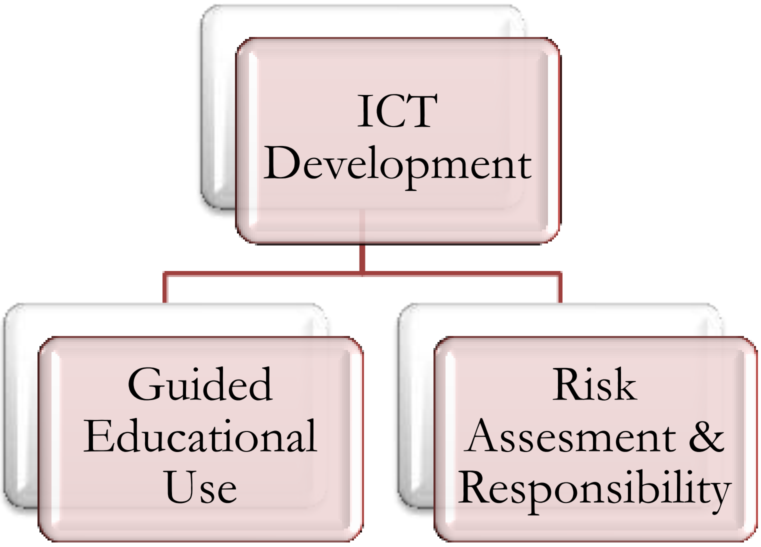


The ICT Policy consists of four main legs, the first will define the educational guidelines of the school in relation to the role of ICT in education and development, the second will describe acceptable usage of ICT resources, the third will define ICT Regulation and the fourth will focus on remedial steps to address transgressions.

2. CORE PRINCIPLES OF ICT DEVELOPMENT

ICT access and usage will be planned to enrich and extend learning and teaching activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. Staff should guide pupils in on-line activities that will support the learning outcomes and skill developments planned for the pupils' age and maturity. Pupils will be educated in the effective use of ICT in research, including the skills of knowledge location, retrieval and evaluation (also refer to Bloom's taxonomy).

The ICT Development guidelines are built on the following core principles:



2.1 GUIDED EDUCATIONAL USE

Curriculum based usage of ICT should be planned, task-orientated and educational within a regulated and managed environment.

While educational benefits should result from this ICT usage these can also include exercises in things like creativity, innovation and exploring. Guided Educational usage could focus on:

- General computer usage
- Usage of network environments
- Usage of the Internet
- Usage of internet resources such as, but not limited to, chat rooms, search engines, online mail resources etc
- Usage of e-mail
- Usage and interaction with social media and social groups

2.2 RISK ASSESSMENT& RESPONSIBILITY

Internet safety at **Blue Hills College** will depend on our staff, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile devices. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions will be judged carefully.

The technology century life presents dangers including sex, violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become "Internet Wise". The ICT Development program will ensure that our students are fully aware of the risks, perform risk assessments and implement remedial and preventative measures to protect against these risks. Students may obtain Internet access in Classrooms, Libraries, public access points and in homes -ideally a similar approach to risk assessment and Internet safety would be taken in all these locations by the students.

3. ACCEPTABLE USAGE OF ICT

3.1 SECURITY

In order to use the school's computers and or tablets each pupil must use their allocated username and password.

Pupils must not use a password belonging to another person, or attempt to access any files where they have not been authorised. **Passwords must remain confidential and pupils must not allow others to access the network with their personal password. Pupils must not gain or attempt to gain unauthorised access to any computer system(s) for any purpose.** Such hacking or attempted hacking is a criminal offence under the Electronic Communication and Transaction Act, Act 25 of 2002. The following is not permitted on school IT equipment(Tablet) without express permission from the Head of IT Services:

- **Games, Music, Video and any other non-school related software's**
- Downloading and/or installing software on school equipment
  - SIM card and memory card

3.2 ANTI-VIRUS

Potential sources of viruses include shared media such as floppy disks, CD-ROMs, DVD-ROMs, USB Memory sticks, email (including, but not limited to, files attached to messages), and software or documents copied over networks and downloaded from the Internet. In order to protect against the virus threat, anti-virus software is installed and updated regularly on all school servers and PCs. Any pupil-owned tablet, PCs, laptops or mobile computing devices connected to the network must have Anti-Virus software installed.

3.3 INTERNET ACCESS AND USE OF ICT

Internet Access

Blue Hills College will avail an internet access to all our students through the library.

All pupils' internet access must be via the School's wired or wireless network and on a device that has been configured by the IT Services department (library & computer lab). ***Accessing the internet via 3G cellular networks on any device (e.g. tablet, laptop, PDA, mobile telephone) is not allowed.*** If special permission is granted to use such, users must adhere to the policies laid out in this document when doing so on the school grounds.

Illegal Activities

Pupils must not, by using any service, possess or transmit illegal material. Pupils should be aware that as the internet is a global network, some activities/material which may be legal in South Africa , may be illegal elsewhere in the world and vice versa. If you are in any doubt as to the legality of anything, don't do it.

File Sharing (Peer to peer networking)

Sharing of files and downloading of files over peer to peer network connections is only allowed when downloading educational content, that is not copyrighted.

Offensive Material

The Internet has excellent educational potential for pupils but is also of major concern with its ease of access to seriously offensive sites. Internet provided throughout the school network is filtered and is monitored and supervised by the school. If you inadvertently come across a site which contains offensive material you must report this matter immediately to your educator or to the IT Service Desk, so that the site can be blocked. Under no circumstances must you mention the site to others. Anyone found attempting to access or in possession of offensive material will be reported and access to the Internet immediately blocked.

It is a criminal offence, even for a learner, 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 to another child.

Social Networking Websites

Access to Social Networking Websites (e.g. Face book, MySpace, Whatsapp, etc) is not permitted at school or during lesson time (except with explicit permission). If such permission is granted, pupils must ensure that any comments or pictures etc. adhere to the school behaviour rules that require pupils to be responsible, thoughtful and considerate and to bring credit to the individual and the school.

Online Email

Access to online email services (such as Hotmail or Google mail) is permitted. Such webmail email services can be used by pupils to correspond with family and friends. However, these services must not be used during lesson times or to download, upload or transfer files that are otherwise restricted.

Internet access via a Proxy

Accessing the Internet via a third party ‘proxy’ website is strictly prohibited at all times.

Instant Messaging (IM)

Use of Instant Messenger clients (such as MSN or AOL etc) is permitted outside of normal school times. Usage must be restricted to basic messaging; voice or video communication is not permitted.

Chat Rooms

Before accessing any Chat Rooms or engaging in any online communications, pupils should familiarise themselves with the potential dangers of online chat and how to keep safe.

Under no circumstances should **Blue Hills College** learners give out any private information.

Streaming Media

Schoolwork-related streaming audio and video media accessed via the Internet (e.g. online radio services and news broadcasts) is permitted, although may be subject to restrictions due to Internet bandwidth limitations. This can only be done after special permission has been granted.

Plagiarism and the Internet

Plagiarism is the theft of ideas and works from another author and passing them off as one's own. Students should be aware that plagiarism is not only cheating but where word per word and sufficient data is copied; an illegal infringement of copyright.

School references

Should pupils directly refer to the school on any internet website, all comments must adhere to the school behaviour rules that require pupils to be responsible, thoughtful and considerate and to bring credit to the individual and the school.

Network Usage

There are Wireless and/or Wired network facilities provided at the school. The facility is provided for study purposes during the normal school day (which includes Private Study classes and Study hours). Wireless connection will be made available to all our learners for use in the classroom and within school premises. This connection will be made available as soon the learner avails a tablet which meets the minimum specifications as recommended by the school. The IT Service Desk will provide the relevant instruction to connect to the Wireless Blue Hills College intranet.

Games

No games; licensed or unlicensed are allowed on School premises and any electronic gadgets(Tablets). The games may only be accessed with permission and for educational purposes.

Removable Media

Use of removable storage media (for example USB keys, SD card) is permitted only where no additional software installation is required and space is limited on tablet.

Portable Media Players

Portable media players (e.g. iPods and MP3 players, including video players) are not allowed. Non-schoolwork related media files must not be stored on the School's network.

Digital Cameras

Digital cameras may be connected to the schools computers for the purpose of transferring schoolwork related images only.

Digital Storage media

Personal pictures files and images (e.g. JPG or BMP files) must not be stored on the network. Personal audio files (e.g. MP3 or WMA files) must not be stored on the network. Personal movie files (e.g. MPG or WMV files) must not be stored on the network or tablets. **School work related media files may be stored on the network.**

Printing

Printing facilities are provided and should be used considerately to ensure minimal waste. Colour printing should only be done when absolutely necessary. No personal printers are permitted. Each pupil will be allow to print for free but with some amount of restriction.

Video Recording

Integrated or attached computer 'web cams' may be used for educational purposes only to record video with prior permission from the persons you are recording and the teacher responsible.

Weblogs/Blogging

A weblog, commonly known as a blog, is a form of online diary or journal. Much like a personal website, blogs give their author a place to air their opinions and comment on current affairs, detail their interests and hobbies, or just post random musings or rants about the world at large. In addition to text, blogs can contain photos, images, sound, archives and related links, and can incorporate comments from visitors.

The process of creating and maintaining a weblog is known as 'blogging', and authors are known as 'bloggers'. Pupils are permitted to contribute to weblogs related to educational issues, but must ensure that any comments or pictures etc. adhere to the school behaviour rules that require you to be responsible, thoughtful and considerate and to bring credit to yourself and the school.

Cyber Bullying

*Cyber bullying is defined as bullying by the use of email, mobile phone and text messages, instant messaging, personal websites and/or chat rooms.*Cyber bullying is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones.

Any suspected cyber bullying (whether during school time or otherwise) will immediately be reported.

Cyber bullying could consist of:

- Repeated e-mails or IMs sent
- Following the child around online, into chat rooms, favourite Web sites, etc.
- Building fake profiles, Web sites or posing as child's e-mail or IM
- Planting statements to provoke third-party stalking and harassment
- Signing child up for porn sites and e-mailing lists and junk e-mail and IM.
- Breaking into their accounts online
- Stealing or otherwise accessing their passwords
- Posting images of the child online (taken from any source, including video and photo phones)
- Posting real or doctored sexual images of the child online
- Sharing personal information about the child
- Sharing intimate information about the child (sexual, special problems, etc.)
- Sharing contact information about the child coupled with a sexual solicitation ("for a good time call …" or "I am interested in [fill in the blank] sex…")
- Reporting the child for real or provoked terms of service violations ("notify wars" or "warning wars")

- Encouraging that others share their top ten "hit lists," or ugly lists, or slut lists online and including the child on that list.
- Posting and encouraging others to post nasty comments on a child's blog.
- Hacking a child's computer and sending a child malicious codes.
- Sending threats to others (like celebrities or prominent people) or attacking others while posing as your child.
- Copying others on a child's private e-mail and IM communications.
- Posting bad reviews or feedback on a child without cause.
- Registering a child's name and setting up a bash Web site or profile.
- Posting rude or provocative comments while posing as a child (such as insulting racial minorities at a Web site devoted to that racial minority).
- Sending spam or malware to others while posing as a child.
- Breaking the rules of a Web site or service while posing as a child.
- Setting up a vote for site (like "hot or not?") designed to embarrass or humiliate a child.
- Masquerading as a child for any purpose.
- Posting a child's text-messaging address or cell phone number online to encourage abuse and increase a child's text-messaging or cell phone charges.
- Launching a denial of service attack on a child's Web site
- Sending "jokes" about a child to others or mailing lists.

3.4 MOBILE PHONES

While the school acknowledges that mobile phones have become an important and useful means of communication, it is also aware of the fact that their use and abuse, particularly by children, pose social, ethical and safety consequences.

The school would prefer students not to have mobile phones in their possession while they are at school or in school uniform for the following reasons:

- Students who carry or use mobile phones in public; particularly when travelling to and from school have become the targets of criminals who accost them and rob them of their mobile phones and other possessions. These attacks occur most frequently when students are seen using their mobile phones, particularly if they are expensive and/or "latest models" of sought-after brands.

- Theft of mobile phones at school from bags and blazers and dormitories is a persistent problem.
- Students are careless with their mobile phones and leave them lying around or in blazer sand bags which are left unattended. Lost and mislaid mobile phones are frequently claimed to be stolen when this is not the case.
- Mobile phones can be used to cheat in examinations and tests. For this reason, no mobile phones are permitted in examination venues or in teaching venues when tests and examinations are written. This same policy applies to the externally set national examinations.
- Mobile phones are increasingly multi-functional, offering an array of features which are designed to attract and entertain users. The ready availability of these features means that students with mobile phones tend to access and use these features in the classroom, becoming distracted from their work. Students with low levels of self-discipline, poor concentration and/or a poor work ethic are more likely to become distracted by these features.
- Mobile phones allow students unlimited access to salacious and age-inappropriate material.
- Mobile phones make students vulnerable to approaches by undesirable individuals or groups including criminals and paedophiles.
- Mobile phones may carry private and personal material, including photographs, video clips, voice messages and personal details which may become accessible by undesirable individuals and groups when mobile phones are lost, borrowed or stolen.

The school will not take responsibility for the theft or loss of any mobile phone brought to school, no matter what the circumstances. This includes the loss or theft of mobile phones that may be handed in to teachers and/or coaches for safekeeping, as well as to mobile phones which have been confiscated from students who use them in defiance of the school rules.

Students who, despite the school's policy, insist on bringing a mobile phone to school are required to ensure that it is:

- turned off (not on "silent") and is not visible while they are in the school building

- is not on their person when they are writing any test and not in the examination venue when they are writing examinations.

The school will not, in principle, under any circumstances engage parents in discussions resulting from complaints parents have received from their children emanating from the use of mobile phone during the school day. A learner who is found guilty of having misused his/her phone within the school premises or outside the school (on matters) relating to the school or other learners, will be dealt with according to the School Code of Conduct relating to misuse of a mobile phone(cell-phone).

4. TABLETS

While the school acknowledges that tablets have become an important and useful means of communication and learning, it is also aware of the fact that their use and abuse, particularly by children, pose social, ethical and safety consequences.

- Theft of tablets at school from bags, blazers and dormitories is a persistent problem and the pupil is encouraged to take up ownership of his or her device.
- Students are careless with their tablets and leave them lying around or in blazer sand bags which are left unattended. Lost and mislaid tablets frequently claimed to be stolen when this is not the case.
- Tablets can be used to cheat in examinations and tests. For this reason, no tablets are permitted in examination venues or in teaching venues when tests and examinations are written. This same policy applies to the externally set national examinations.
- Tablets are increasingly multi-functional, offering an array of features which are designed to attract and entertain users. The ready availability of these features means that students with tablets tend to access and use these features in the classroom, becoming distracted from their work. Students with low levels of self-discipline, poor concentration and/or a poor work ethic are more likely to become distracted by these features.

The school will not take responsibility for the theft or loss of any tablet at school, unless the school was responsible in the circumstances. This includes the loss or theft of tablets that may be handed in to teachers and/or coaches for safekeeping, during school programmes.

5. REGULATION

The use of ICT resource brings with it the possibility of misuse as well the inherent dangers including sex, violence, racism and exploitation. It is therefore the aim of this policy to regulate how students utilize ICT resources, what content they access as well as their interaction with other ICT users. As with any other regulation this will be done within the framework of inter-alia the Constitution of South Africa, the laws that govern our country, the policy of the school as well as all applicable social and ethical standards. As such transgressions of the policy must be dealt with in accordance with the prescribed remedial steps.

Misconduct in relation to the usage of ICT could constitute a minor breach of school policy; it could constitute a socially embarrassing incident, or a criminal act, breach of a person's constitutional rights or even cause an international incident.

Misconduct in relation to ICT could be a breach of the following Acts and could constitute a civil or criminal transgression:

- Infringement of a person's constitutional rights in relation to dignity, respect, right to privacy etc
- Hate speech or racist comments
- Illegal access to information
- Illegal interception of communication
- Harassment
- Slander
- Defamation of character
- Fraud & Corruption
- Extortion
- Copyright & Plagiarism
- Transgressions into child pornography

In relation to a breach by or against a student of any of the above transgressions the school, its employees, parents and students have a legal obligation to report it to the authorities. Failure to do so could constitute a criminal offence in itself.

6. REMEDIAL ACTION

Monitoring

Blue Hills College has the obligation and right to monitor record and copy any and all utilisation of the ICT infrastructure of the school for the purpose of ensuring that the school rules are being complied with and used for legitimate purpose.

If a student chooses to bring his/her own ICT device, including mobile phones or devices, to school, the school has the right to monitor, record, copy any and all utilisation of the such ICT devices for the purpose of ensuring that the school rules are being complied with and used for legitimate purpose.

Remedial Process

Situations will exist where the school will have to take action against a student for breaching the ITC Policy, or to protect the student against external transgressors or to protect a student against another student. In all these situations the school will act in a correct and decisive manner. The process of doing this will be clearly defined and communicated to all staff, students and parents. At all times it must be clear that the school will act in the interest of justice and in the interest of the student.

If a transgression is reported or suspected, the school will take the necessary actions which may involve all or some of the following; monitoring, recording, copying or taking possession of any ICT device, whether private or property of the school. The said device will be accessed by the school, representative of the school or person appointed by the school to establish the validity of the suspicion or report.

A charge will be compiled based upon the facts established and the necessary action will be taken against the student.

The school will endeavour to resolve all matters with the utmost care and confidentiality and to resolve all matters in an agreeable manner, if possible, internally.

If there is a legal obligation on the school to report any action to the authorities, the school will endeavour to do so with the utmost care and confidentiality.

The parent or guardian of any student involved in any transgression will be contacted and notified prior to any action been taken.

Adherence and Consent

In accepting the Blue Hills College's ICT Policy you undertake to adhere to the rules of the school and consent to the school authority to take the necessary actions by monitoring, recording, copying, accessing or taking possession of any ICT device, whether private or property of the school which is misused.

7. INTERNAL REMEDIAL ACTION (PUNISHMENT)

With all the above mention offenses, a learner will serve series of instant punishment to serve as a corrective measure for the student. The detention of the leaner will be as follows:

- A student may do some 300 bricks work as a first time IT offender and may pay a fine of R50 to get his or her books reloaded into the tablet and tablet will be formatted.
- A student may do 650 bricks work as a second time IT offender and may pay a fine of R50 to get his or her books reloaded and tablet will be formatted.
- Minor offenses (games and use of ear/head phones) may attract lesser punishment like a fine of R50 to get books reloaded back on the tablets and tablets will be formatted.

Date ___________

Student Name ________________________ Signature _________________________

Parent Name ________________________ Signature _________________________

Parent Name ________________________ Signature _________________________