GLEN AUSTIN HIGH SCHOOL
DEVICE POLICY

INDEX

INTRODUCTION

Glen Austin High School has introduced a "BOYD" initiative with effect from January 2015. This policy is intended to cover relevant aspects of that initiative and may be subject to amendment in the future.

DEFINITIONS

BOYD ……. "Bring Your Own Device"

Device ….. Learner's own IPAD or TABLET or CELLPHONE or SPEAKER.

ICT ……. Information Communication Technology

School ….. Glen Austin High School

Learner … Learner of Glen Austin High School

User …….. Any person using or accessing any of the School's ICT facilities

RESPONSIBILITY

Learners are expected to demonstrate appropriate and responsible behavior when using the School's ICT facilities as well as when using their own personal Devices.

Students are expected to comply with the specified guidelines and rules set out below. Necessary disciplinary action will be taken against Learners who disregard this policy.

Learners bring their Devices to use at Glen Austin High School at their own risk.

Learners are personally responsible for keeping their Device up-to –date and secure. The installation of tracking software is compulsory.

Glen Austin High School is no way responsible for:

- Maintenance of any Device.
- Broken Devices.
- Lost or stolen Devices.

TERMS AND CONDITIONS

- The use any Device and/or the transmission of any electronic material in any form that is in violation of ant South African legislation or regulations as well as International Law or any of the School's rules is strictly prohibited. This includes, but is not limited to, copyright material, threatening, obscene or offensive material, or material protected by trade secret.
- The use of the School's ICT facilities is a privilege and not a right. Abuse of such facilities will result in the withdrawal of access from all ICT facilities.
- Learners are personally responsible for their actions in accessing and utilizing the ICT facilities of the School.

MONITORING

- All activities utilizing the School's ICT facilities are monitored and logged.
- The School reserves the right at all times to determine whether usage of the School's ICT facilities is appropriate. This includes the right to review, amongst others, Internet usage, material held in user accounts and server space.
- In reviewing and monitoring user accounts and file server space, the School will respect the privacy of the user accounts at all times.

- The School reserves the right to inspect any Device and take the appropriate disciplinary action in the event that either the Device or any material contained on the Device, has been or is intended to be used for, any illegal or unlawful activity.

INTERNET ACCESS

- No Learner will be granted access to the Internet via the School's Wi-Fi network.
- Access to Social Networking websites (e.g. Facebook. Myspace etc.) is not permitted through the School's network.
- Email services must not be used to download, upload or transfer files that are otherwise restricted, prohibited or contain any offensive or illegal material.

SECURITY

- Each Learner will be issued with a unique and specified password and/or other access details for each ICT system at the School that they are permitted to access.
- Password and/or other access details are to be kept strictly confidential and are to be used by the Learner to whom they are issued.
- No Learner may attempt to use any password or other access details belonging to any other person to access any of the School's facilities.
- Learners are prohibited from attempting to access any files, folders or similar which they have not been authorized to access.
- Learners must not attempt to, nor gain any unauthorized access to any of the School's ICT facilities or systems for any purpose. Such hacking or attempted hacking is a criminal offence under the Electronic Communication and Transaction Act, Act 25 of 2002.
- Any attempt to access any of the School's ICT Facilities posing as "System Administrator" will result in the cancellation of User privileges and the implementation of disciplinary procedures against that person.
- No Learner may use another Learner's account.
- No passwords may be shared amongst Learners.
- Learners may not modify computer files, folders or settings on any of the School's ICT facilities without prior authorization from an IT staff member.

ILLEGAL ACTIVITIES

- Learners must not, by using the School's ICT facilities, possess or transmit any illegal material of any nature or form. (Note – As the Internet is global, some activities/material which may be legal in other countries, may be illegal in South Africa and vice versa)

REGULATIONS

Misconduct in relation to the usage of ICT facilities could result in the person who performed such misconduct being legally prosecuted for a variety of criminal offences, or being subjected to civil claim for damages, or both. Examples of such infringements are:

- Infringement of a person's constitutional rights to dignity, respect, privacy etc.
- subjecting a person to "Hate Speech" or racist comments
- Illegal access to information
- Illegal interception of communication
- Harassment
- Slander
- Defamation
- Fraud & Corruption
- Extortion
- Copyright & Plagiarism
- Sexual and pornography offences.

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

OFFENSIVE MATERIAL

- If any person inadvertently accesses any web-site containing offensive material such person must immediately report it to the IT Service Desk, so that the site can be blocked.
- Under no circumstances must the name or URL of the site be disclosed to other Learners or Staff.
- Any person found attempting to access, or to be in possession of, offensive material, will have their Wi-Fi and Internet blocked, and in addition, will be subjected to the School Disciplinary Process.

➢ **It is a criminal offence, even for a child, to create, download, possess, distribute or display any child pornography.**

➢ **It is also a criminal offence to display or distribute any pornographic material to any child even if the person displaying or distributing such pornographic material is a child themselves.**

CYBER BULLYING

Cyber bullying is illegal and is strictly prohibited.

Cyber bullying occurs when any person is tormented, threatened. Harassed, humiliated, embarrassed or otherwise targeted by another person using any form of ICT facility.

- Any person is subjected to cyber bullying must report it immediately to their Grade Head or Deputy Principal.
- Any person who is aware that another person is engaging in, or is the target of cyber bullying, must report it immediately to their Grade Head or Deputy Principal.

➢ **Examples of cyber bullying are contained in Annexure A. Note that this is not an all-encompassing list and other actions may also constitute cyber bullying.**

CLASSROOM PRACTICE

- All devices are to be used for educational purposes only during lesson time.
- If a Device is left at home or is not charged, the Learner remains responsible for completing all schoolwork as if they had use of their Device.
- Learners are responsible for ensuring their Devices fully charged before the start of the School day.
- Devices should be brought to School each day unless an Educator instructs otherwise.
- Sound must be muted at all times unless permission is obtained from the Educator.
- Games are not to be played during ant curriculum activity.
- Learners must ensure that they do not loose work due to mechanical failure accidental deletion. Device malfunctions are not an acceptable excuse for not submitting work. Educators and the IT department will instruct Learners on methods of managing workflow.
- Use of Devices during the school day is at the discretion of Educators and Staff. Learners must use devices as directed by their Educator.
- The use of a Device is not to be a distraction in any way to Educators or Learners and may not disrupt teaching in any way.
- Learners may not use their devices to communicate with each other during class time, such as email, chat messaging and similar.
- Learners should always turn off and secure their Device after completing their work to protect their information.
- The use of a “lock” password is compulsory.

GENERAL

Any Learner who attempts to hack or interfere with any other account, including any attempt to break into the network, spread viruses or change any directory permissions will be permanently denied access to the School's Wi-Fi and will be subjected to the School's disciplinary process as well as a criminal case possibly opened against him.

- Learners are prohibited from attempting to bypass blocked sites by any means whatsoever. Any attempt will result in the Learner being blocked from the school's Wi-Fi network and subjected to the School's Disciplinary Process.
- No printing is allowed at the school.
- No Learner is permitted to download or copy any copyrighted or otherwise protected material onto their Device.
- Learners may not play or download games or watch videos or movies via the Internet.
- Using offensive language when transmitting to any other Learner or a member of the School's Staff is prohibited – this includes impolite, anti-social, profane, abusive, racist, or sexist language.
- Learners must not use their Device's camera to take images/videos of ant Learner or educator that may be deemed to be inappropriate in any manner. Doing so may expose the Learner taking such images/videos to criminal or civil action.
- Inappropriate media may not be used as a screensaver or background on any Device, including pornographic images, pictures of violence, inappropriate language, alcohol, drug, racist or gang related symbols or pictures.
- No Devices will be allowed into an examination/test venue. Learners are discouraged from bringing Devices to school during examinations or tests.
- Should a Learner bring a device during examinations or tests, it is their responsibility to store the Device outside the examination or test venue.
- Using the Device to listen to music in class or whilst walking around the school is forbidden.
- Use of Devices to play music is only allowed on the Sports Field, away from the buildings area. Volume must be moderate and not reach the buildings area.
- Images or movies of people are not to be shared in a public space on the internet, without the permission of the individual concerned or a staff member.

- If a Learner logs on to IT School Innovation server with a login that is not your own, your tablet will be denied access for a certain period of time.
- No Educator or Councilor will take responsibility for the security 0f the Device.
- No device may be opened or used during the assembly.
- Should any person outside the School access the School's network via a Learner's login details, the relevant Learner will be suspended from the Wi-Fi pending a Disciplinary Enquiry and the Scholl will open a criminal case against the guilty party.
- Devices belonging to other persons are not to be tampered with in any manner.
- Any device found unattended must immediately be handed in at Reception or the IT desk.

CONSEQUENCES FOR BREACHING DEVICE POLICY

If a Learner continues to disregard the rules contained in this Policy after one warning, the following will apply.

- Parents will be notified BEFORE the Learner can redeem the device.
- Access to the Wi-Fi network will be denied to the Learner.
- The Device will be confiscated and placed in the front office for parents or learner to collect once a cash amount of R200.00 has been paid at the front office and a receipt issued.
- Cell phones and speakers will be held for a period of ONE WEEK before a learner can collect, in addition to the payment of the R200.00.
- Tablets can be collected as soon as the amount of R200.00 is paid.
- The Learner will be banned from using a Device at School for a period of time commensurate with the severity of the offence.
- Detention will be implemented.
- Depending on the circumstances of each matter, a Learner may be subjected to the School's disciplinary process and a criminal charge may be laid.

I have read and understood the Glen Austin High School DEVICE POLICY 2014 and agree to fully

obey.
In accepting the School's DEVICE POLICY 2014, I undertake to adhere to the rules of the School and accept the authority of the School to take the necessary actions by monitoring, recording, copying, accessing or taking possession of any Device in order to protect the integrity of the School's ICT facilities and/or the protection of any Learner.

DATE _____

STUDENT NAME _____

STUDENT SIGNATURE _____

PARENT NAME _____

PARENT SIGNATURE _____

ANNEXURE A

Examples of Cyber-Bullying

- Repeated emails or Instant Messages (IM) sent.
- Following a person online, into chat rooms, favorite websites, etc.
- Building fake profiles, websites or accessing another person's email or IM.
- Issuing statements to provoke third-party stalking and harassment.
- Signing a person up for porn sites, emailing lists, junk email and IM.
- Breaking into a person's online accounts.
- Stealing or otherwise accessing a person's passwords.
- Posting an image of a person online.
- Posting real or doctored sexual images of any person online.
- Sharing personal and/or intimate information about a person online without their permission.
- Encouraging the inclusion of any person on any derogatory "hit list" such as, but not limited to, "ugly lists", "slut lists" and similar.
- Posting or encouraging others to post nasty comments on a person's blog.
- Hacking a person's computer and sending a person malicious codes.
- Sending threats to or attacking others, including while posing as another person.
- Copying others on a person's private email and IM communications.
- Posting bad reviews or feedback on a person without cause.
- Registering a person's name and setting up a bash website or profile.
- Posting rude or provocative comments while posing as another person.
- Sending spam or malware to others, including while posing as another person.
- Breaking the rules of a website or service while posing as another person.
- Setting up any "vote" (e.g. "hot or not") designed to embarrass or humiliate any person.
- Masquerading as another person for any purpose whatsoever.
- Posting any person's contact details online to encourage abuse or harassment or other prejudice to that person.
- Launching a denial of service attack on any website.
- Sending "jokes" about a person to others or mailing lists.

ANNEXURE B

DEVICE CARE

The following general guidelines are recommended:

- Use protective covers/cases
- Never drop or place heavy objects on top of the Device. Do not “bump” the tablet against lockers, walls, car, doors, floors, etc. as it will eventually break the screen.
- Use a soft cloth to clean the Device screen.
- Do not subject the Device to extreme heat or cold.
- Do not leave the Device in the sun.
- Do not place anything in the carrying case that will press against the cover.
- Do not drop the Device.
- Keep the Device away from liquids.
- Keep the Device away from magnets.