Cedarwood School

113 - 117 Dunmaglass Road, Glenferness

Prep Switchboard: 011 465 9830
Emergency: 071 609 7253

College Switchboard: 011 467 4889
Emergency: 072 617 5291

www.cedarwoodschool.co.za

CEDARWOOD SCHOOL
IT Policy – Pupil Contract

This policy must be read in conjunction with the POPIA Manual

Purpose of the Policy
Learners are responsible, personally, for their actions in accessing and utilizing the school's computer resources. Learners are expected never to access, keep or send anything that they would not want their parents or teachers to see. Learners are expected to demonstrate appropriate behaviour when using the school's computer facilities, just as they do when they are in a classroom.

Communications on the Internet are often public in nature and general school rules for behaviour and communications therefore apply. The use of the computer facilities is a privilege, not a right, and may be revoked if abused. It is expected that users will comply with the specified standards and rules set out below.

UNACCEPTABLE USES:
The following behaviour or uses are unacceptable and punishment will be given to offenders. This punishment can include the learner's computer access being removed for a period of time, the learner access to certain programmes being removed, as well as suspension from class depending on the seriousness of the infraction. For vandalism, the learner will be responsible for any financial costs that might occur.

- Using language that is considered offensive in anything you type or send. This includes impolite, anti-social, profane, abusive, racist, or sexist language.
- Cyber-bullying of any form, whether via e-mail, SMS or social network sites such as Facebook, Instagram etc
- Entering chat rooms / chat applications (e.g. Skype) or access sites that have no relevance to the project on which the learner is working.
- Attempting to access pornographic or sexually explicit material of any kind, via e-mail or any other internet facility. Learners attempting to access unacceptable sites will be excluded from the centers for one month or longer, depending on the severity of the offence. A letter will be sent home informing parents of the site visited and this letter will be kept on record. Parents will have to send in a reply slip and may be called in for an interview to view the sites that their child was attempting to access.
- Sending or re-sending chain letters.
- Mail-bombing another person's e-mail account. This is bullying and will be punished accordingly.

- Using anyone else's login and thereby impersonating and possibly incriminating another user. This is fraud, which is a criminal offence.
- Attempting to hack into or interfere with any other account, including any attempt to break into the network, or spread viruses or change the permissions on any directory.
- Attempting to bypass any sites by any means whatsoever that have been blocked by the administrator.
- Copying any games or other unauthorized software onto any part of the network including your personal directory. Pirating of software is a criminal offence, and no shareware software is allowed unless it is approved and installed by the Network Administrator.
- Tampering with equipment or moving equipment from the labs or classrooms. No-one may be in possession of any school computer equipment without the written permission of the Administrator.
- Online email is not permitted.
- Pupils will not have access to the school network unless specified requested by a teacher for a specific period of time.
- Vandalising any equipment. Learners will be expected to pay for any costs incurred through deliberate damage to computer equipment.
- Unauthorised games may not be played on the computers at any time. If a learner is caught playing any games, his or her computer privileges will be suspended for a time period.
- The use of the internet during class time, without permission, is unacceptable. If the work set has been completed, permission may be asked to work on the Internet. If learners misuse this privilege, internet access will be blocked for use at all times and the privilege removed.

1. INTERNET ACCESS AND USE OF ICT

Internet Access

All pupil internet access must be via the School's wired or wireless network and on a device that has been configured by the IT department.

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 the SA, 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.

Downloading

Certain restrictions may be implemented to prevent file downloads at certain times. Downloading certain file types can introduce viruses and other security threats onto the network; therefore, some file types may be blocked by default. Contact the IT Team to download any essential files you require that have been blocked.

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 access 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 teacher 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 child, 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 a child.

Social Networking Websites

Access to Social Networking Websites (e.g. Facebook, Myspace, Instagram) is not permitted.

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) is permitted outside of normal school times. Usage must be restricted to basic messaging; voice or video communication is not permitted.

Chat Rooms

Access to Chat Rooms is not permitted.

Streaming Media

Schoolwork-related streaming audio and video media accessed via the Internet (e.g. online radio services and news broadcasts) is not permitted.

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 sufficient content 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 wired network facilities provided at the school in the IT Labs. The facility is provided for study purposes during the normal school day. To request connection, you should contact the IT Team who will provide the relevant instructions.

Removable Media
Use of removable storage media (for example USB sticks) is permitted when access is given by the IT Department.

Digital Storage media
Personal picture 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. School work-related media files may be stored on the network.

Cyberbullying
Cyberbullying is defined as bullying by the use of email, mobile phone and text messages, instant messaging, personal websites and/or chat rooms. Cyberbullying 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 will immediately be reported.

Cyberbullying could consist of, but is not limited to:

- ✓ Repeated e-mails or IMs sent
- ✓ Following the child around online, into chat rooms, favourite Web sites, etc.
- ✓ Building fake profiles, Websites or posing as child's e-mail or IM
- ✓ Planting statements to provoke third-party stalking and harassment
- ✓ Signing 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 code.

- ✓ Sending threats to others (like the president of the United States) or attacking others while posing as a 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.

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 pupil 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

The school 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.

Remedial Process

Situations will exist where the school will have to take action against a student for breaching the ITC Policy.

If a transgression is reported or suspected, the school will take the necessary actions by 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, a representative of the school or a 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 pupil.

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 pupil involved in any transgression will be contacted and notified prior to any action being taken.

Adherence and Consent

In accepting the School'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.

_____	_____	_____
Date	Pupil Name	Signature
_____	_____	_____
Date	Parent Name	Signature
_____	_____	_____
Date	Parent Name	Signature

Date	Page no, heading, brief description of changes	Entered by
15/05/18	Spelling	Management
18/07/18	None	P Kotze
26/09/18	Spelling and words taken out	Team(Review File)
30/09/19	Words taken out adding of some words	D Bruwer
11/09/20	POPIA	Management
11/09/21	None	Management
21/09/22	Various	IT Department
22/11/23	None	IT Department