CEDARWOOD SCHOOL

IT Policy – Pupil Contract

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.
- 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 centres 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.

- Vandalising any equipment. Learners will be expected to pay for any costs occurred 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 privilege 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. SECURITY

In order to use the school's computers and systems, 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 without express permission from the Head of IT Services:

- Changes to installed software or hardware configurations
- Downloading and/or installing software on school equipment

2. ANTI-VIRUS

Potential sources of viruses include shared media such as 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 PCs. Any pupil-owned PCs, laptops or mobile computing devices connected to the network must have Anti-Virus software installed.

Any device that is found not to have Anti-Virus software, or that does not have a recent update, will be removed from the network until remedied.

3. 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 Services department. Accessing the internet via 3G cellular networks on any device (e.g. computer, PDA, mobile telephone) are allowed but 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 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

The school's Internet access has a finite bandwidth and can become slow and unresponsive under heavy usage, particularly when file downloads is being performed. This can prevent other users from performing their work. For this reason, 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 Service Desk to download any essential files you require that have been blocked.

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 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) is not permitted.

Online Email
Access to online email services (such as Hotmail or Google mail) is permitted, but not during lesson time (except with explicit permission). Although, 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. Such webmail email services can be used by pupils to correspond with family and friends. However, these services must not be used 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) 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 permitted, although may be subject to restrictions due to Internet bandwidth limitations.

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 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). To request connection, you should contact the IT Service Desk who will provide the relevant instructions.

Games

Licensed and approved games are allowed on School PCs and network at specific times and under supervision. While they are also allowed on mobile devices they must only be accessed with permission.

Removable Media

Use of removable storage media (for example USB sticks) is permitted only where no additional software installation is required and a full virus scan has been performed by the IT Service Desk.

Portable Media Players

Portable media players (e.g. iPods and MP3 players, including video players) may be connected to the School computer network for school work use only. Non-schoolwork related media files must not be stored on the School's network.

Digital Cameras

Digital cameras may be connected to the school's 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. School work related media files may be stored on the network.

Voice over IP

Voice services (e.g. Skype or MSN Messenger) are currently permitted on approved parts of the school's computer network and devices.

Printing

Printing facilities are provided and should be used considerately to ensure minimal waste. Personal printers are permitted and each pupil will be responsible for consumable supplies and maintenance of these.

Video Recording

Integrated or attached computer 'webcams' 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, 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, 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, Web sites 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 codes.
- ✓ 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.

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 is a persistent problem. Students are careless with their mobile phones and leave them lying around or in blazers and 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 pedophiles.
- 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 must 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. Parents sign a form that pupils handed in the phones at own risk. No responsibility taken by the teacher.

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

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, or to protect the pupil against external transgressors or to protect a student against another student. In all these situations the school must act in a correct and decisive manner. It is therefore necessary that the process which must be clearly defined and communicated with all staff, pupils and parents and that it must be clear that the school will act in the interest of justice and in the interest of the pupil.

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, 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 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 been 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

RECORD OF CHANGES

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)