EVERSDAL PRIMARY SCHOOL

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

CONTENT

Information- and Computer Technology

Introduction

This document is the policy for the Information and Computer Technology Systems, as well as the Social Media of Eversdal Primary School as approved by the Governing Body of the school, on 11 August 2014. This policy was written in accordance with The Constitution of South Africa, 1996; the South African Schools Act 84, of 1996; Regulation 27 of the National Education Policy of 1996; applicable Provincial Regulation with regard to school education, and the Law Regulating the Interception of Communication and the Provision of Communication Related Information 70 of 2002.

The aim of the policy is to regulate the use of the school's Information Systems with regard to the communication of any information, as well as the applicable use of social media platforms by educators, non-educators, and learners. The school acknowledges the development of social media as a means of communication, but at the same time realises that it can only be used optimally if it is used responsibly.

The school respects the privacy of the educators, non-educators and learners. However, this privacy does not include their work-related conduct or the use of the equipment, resources or supplies of the school.

According to the the Law on the Regulation and Interception of Communication and the Provision of Communication Related Information 70 of 2002, any person may intercept any communication in the instance where they are party to the communication, unless said person is intercepting the communication for unlawful activity.

The school may thus intercept any communication which is sent through the school's Information Systems or Social Media platforms, as well as any school related infomation.

Application

This policy is relevant to all users of the school's Information and Computer Systems. It also applies to the voicing of opinions and commenting on social media by educators, non-educators and learners who may, in any way, be associated with the school. Any person who works with the Information System within the school structure is accountable for the information which is documented in this policy.

Terminology

BYOD – Bring Your Own Device. The name of the system which allows learners to bring their own device to the school. This includes tablets, cellphones, etc.

Information System – the system which consists of all communication channels which are used in the school.

ICT – Information and Computer Technology.

Intercept – the acquiring of the content of auditory, or any other, communication in any manner to make it available to someone other than the sender or intended recipient and includes the-

(a) monitoring of any such communication by means of a monitoring apparatus;
(b) view, investigate or inspect the content of any indirect communication; and
(c) divert any indirect communication to another destination, other than the intended one.

School – the Governing Body as well as any person to whom authority or a specific function has been assigned in accordance with this policy.

School management – the headmaster or a member of the school's staff to whom the headmaster delegated authority.

.

Social media – the means of interaction between people during which they create information and ideas which they share and exchange in virtual communities and networks. Social media may include text, audio material, video material, visual material, podcasting and other multimedia communication.

System hardware – any mechanical or electrical apparatus which is connected to the computer system, including the central processing unit and additional or subsidiary apparatus such as printers and external disc drives.

System software – computer software which was designed to run, and manage, the computer hardware and provides a platform on which application software can function.

General

The school's computer and communication systems are generally for official use only. Nonetheless, occasional personal use is allowed in the instance where the no more than a fraction of the number of resources are used which would otherwise be used for official use; does not interfere with productivity; does not distract from school activities; does not cause distress, legal or moral problems for the school's – as well as other – educators, non-educators and learners.

All system hardware and software is the property of Eversdal Primary School. The school is the legal owner of the content of all the files which are stored on its computers and network systems, as well as any messages which are sent by means of these systems. The school reserves the right to access this information without prior concent where there is an operational need to do so. No educator, non-educator or learner, may copy, on any given time or circumstances, any information or data that is stored on the network for personal gain. Information and data that is stored on the server may not be shared with any instution without prior conscent of the principal.

The school reserves the right to audit the systems from time-to-time to ensure this policy is adhered to. The school may, according to its own discression, investigate, move or delete files,including electronic mail(e-mail), for maintenance purposes or in the instance where the files are disrupting the system, whether purposefully or not. The school strictly prohibits the use of illegally acquired media on the systems – this includes the use and distribution of pirated movies.. The school gives no guarantee, categorically or implied, for the services it provides.

The school will not be held responsible for any damage suffered on this system, including the loss of personal data due to system interruptions or the irresponsible use of the system. It stays the individuals' responsibility to make backups of his/her documents that is stored on his/her computer, as well as the data on the iPad. The school is not liable for any offensive material which any user may access through the school's system.

Internet Policy

Internet access is available to all Eversdal Primary School's employees where there is a justifiable need. All internet connections will be provided by the approved internet provider. All other connections are prohibited. It includes any 3G connection on the device. The only form of internet connection that the learners may use during school hours will be supplied and regulated by the school in the form of Wi-Fi.

Internet usage is a privilege which implies the acceptance of responsibilities and the compulsory submission to the states policy and laws. Acceptable use must be legal and ethical and must respect intellectual property, ownership of data, system security mechanisms, individual rights of confidentiality and freedom from intimidation, harassment and offence.

Users will be subject to limitations on their internet usage, as determined by the applicable authority who is in charge. Web content filters will be used to protect the school from improper and indecent material and to limit band width.

Software which filters content will be used to block access to web sites which do not fall within the activities of the school. All web sites containing sexually explicit, as well as indescent and possibly offensive material, will be blocked by means of the WCED web content filter.

The school management reserves the right to investigate the cache files, e-reader, e-reader bookmarks and any other information which is stored on, or accessed through, the school's computers, without prior consent. In this manner, management's access will insure compliance to the internet policy, help with internal investigations and assist in the management of the school.

E-mail policy

The school does not guarantee the privacy and confidentiality of any e-mail.
E-mail usage which violates this, or any other policy, is prohibited. Any e-mail which does not reflect the image and reputation of the school is prohibited.

The user carries sole responsibility for all communication via their designated e-mail address. In e-mails, the concealment or misrepresentation of names, addresses or affiliations is forbidden.

The use of e-mail for commercial purposes is forbidden. Using e-mail with the purpose to abuse, to threaten or offend, is forbidden. E-mail forms part of the management and administrative history the school and may therefore be subject to inspection.

Hardware

The long-term planning must be evaluated and adjusted annually, with regard to the replacing of hardware. The replacement of hardware must take place in consultation with the Financial Committee of the Governing Body, within the predetermined annual budget.

Hardware which is replaced, which no longer satisfies the requirements but is still in a working condition, must be deployed to areas where it is usable or donated as the school sees fit. The IT Inventory must be kept up-to-date with a record of all hardware and guarantees.

In consultation with School Management, an effort must be made to provide the school with the newest technology, in so far as finances permit. Maintenance of hardware will be done internally; however, when necessary the support of an external company may be contracted in.

The ICT inventory contains 'n replacement cycle for all iPads and computers in the school. This cycle entails that all computers will be granted a lifetime of 7 years before

replacement. Every year new computers and iPads will be bought to replace the older models. These replaced computers and iPads will then be written off for tender, where-after it can be donated if a tender isn't received. The new computers will be installed in the computer labs. The computers that are replaced will in turn replace the computers in the classrooms. This ensures that our learners get to work on the newest technology at all times.

Software

Software programs are installed by the IT Department, ahead of time, according to the needs as determined by management. No unlicensed software may be installed by the user. Where the user has a need for a licensed software for school use, it must be installed by the IT Department.

Software may not be deleted or deactivated without prior consent from the IT Department. Software may not be copied and used outside of the school. In the instance where the user requires the software for preparation at home, the steps as prescribed by the Departmental agreement with the supplier must be followed.

All software installed on the system must be licensed. Software must be evaluated and upgraded in order to insure the system remains relevant.

A record of all the license agreements, as well as software licenses, will be managed, updated and filed by the IT Department.

Prohibited activities or behaviour

The following activities and/or behaviour are prohibited:

- The copying of material which is subject to copyright or patent, without appropriate licensing or permission.
- The use of the school's information systems for political gain, personal gain or commercial purposes.
- The copying or removal of software from the school's computers.
- The downloading of material from the internet which is not related to official school activities or business.
- The installing of system hardware or software by unauthorised staff. Unlicensed software, private software, games, public domain software, freeware, shareware or demonstration software may under no circumstance be loaded on official computer equipment without the written concent of the Governing Body.

- The use of personal social media during school hours for personal reasons. This includes, but is not limited to Facebook, Twitter, Instagram or any other social media platform.

- The use of the school's information system for offensive or abusive material is prohibited. The following is considered to be computer abuse:

  - Using the computer to annoy, scare, intimidate, threaten, repulse or to upset through the use of foul language, pictures or other material, or to convey threats of physical or psychological harm to the receiver;
  - Using the computer to continuously contact a person with the purpose of annoying, abusing, or to upset, regardless of whether any real message is conveyed, and/or where there is no justifiable need for communication, and where the receiver requested that the communication be terminated;
  - Using the computer to continuously contact a person with regard to a matter where there is no legal right to do so, subsequent to the receiver giving fair notice that he/she no longer wishes to receive such communication;
  - Using the computer to disrupt or cause damage to the academic research, administrative or related endeavours of the school or another person;
  - Using the computer to violate the academic or any other privacy of a person, or to use it to threaten the person; and
  - Material which is sexist, racist and/or violent.

- The viewing or sending of any material which violates any national, provincial or international law.

- The use of the school's information system to gain unlawful access to any other system or data.

- The gaining of access to and/or the downloading, saving or sending of indecent material via the school's computer system.
- Every educator and non-educator will receive access to information in so far as is necessary to fulfil his/her delegated function, but will not receive access to information which would otherwise be protected unless and until such time that access is deemed necessary and official permission is granted. Authorised users are responsible for the security of their password and profile.

Cyber misconduct

The following forms of cyber misconduct is prohibited:

- Cyber browsing and the misuse of the employers' resources: educators, non-educators and learners may not use the school's resources e.g. computers, telephones, etc., for private use during or after school hours, thereby misusing the work relationship.

- The creating of discord and the spreading of offensive or insulting material: educators, non-educators and learners may not distribute racist, slanderous, sexist or pornographic information. This is considered serious misconduct. Racist comments are not only repulsive, but result in discord.

- Derogatory remarks: educators, non-educators and learners may not distribute or publish insulting and offensive messages about the school, the staff or the learners. Anyone who contravenes may be found guilty of putting the school's name in disrepute, which may lead to disciplinary or legal action being taken.

- Breach of confidentiality: educators, non-educators and learners may not use the school's information system or social media platforms in any way which may tarnish the confidentiality of the school.

- Educators, non-educators, learners and parents who use social media for official and non-official purposes, should note the following: the approved social media sites may only be visited for official purposes when the school's information system is used.

- The message the school wants to convey to all other users, must be well defined.

- Publications must be legal, ethical and respectful. Educators, non-educators and learners may not partake in online communication which may tarnish the name of the school.

- Personal information of educators, non-educators, learners and parents may not be disclosed. Educators, non-educators, learners and parents must note that the school may, from time to time, share photographs which were taken at official school activities on social media sites. People may then be tagged. Users of these social media sites are advised to revise their security settings. Educators, non-educators and learners are advised to block other users from accessing their profile, where they do not know the other user or do not want to be associated with them.

The school accepts no responsibility or liability for poor security settings on the social media profile of any person associated with the school. In the event that an educator, non-educator, learner or parent publishes a comment, photograph or video on any social media platform which could tarnish the name of the school, and a connection to the school is made or is identified or admitted, such person will be subject to disciplinary and legal steps. Legal steps may also be taken against a parent who places the school in disrepute.

All information which is published, must be accurate and confidential information may not be disclosed. Copyright must be adhered to. Only the official, approved logo of the school may be used.

Statements in the media must first be approved by the Governing Body. All privileges, in so far as the school's information system is concerned, will be terminated once an educator or non-educator is no longer employed by the school, or where a learner leaves the school. The school reserves the right to withdraw the privileges of any user at any given time.

Behaviour which interferes with the normal and proper functioning of the information systems, has a negative impact on others' ability to use the information system, or is damaging or offensive to others, and is prohibited.

Server security

Where possible, all servers which store data and applications will be placed in a physically safe environment with strict access measures in place. All server rooms will be regarded as high risk security areas, with strictly controlled access. All servers will be equiped and protected with the newest, approved anti-virus.

Additional programme improvements and updates will be undertaken regularly by the appointed IT service provider of the school, or the school's IT specialist, when necessary.

Only an authorised administrator will receive administrative rights for the servers. Administrative passwords will be confidential and only those staff who are nominated by the school will have access to them.

All critical management or administrative data on the local hard drive of computers must be stored under "Public-staff". Where possible, if the user is in a location where there is no access to the school's network, the data must be copied at the first available opportunity. The user will exercise the sole responsibility to back up data security and maintain it.

Eversdal Primary introduced a new VPN system to it's staff. This gives the educators the opportunity to access the network from home. For protection of the VPN system, it stays the educators responsibility to protect their login details at home and the school. The VPN system will be locked during holidays to limit the risk. The VPN will only be available if the network setup permits it.

Servers will be backed up on a weekly basis by the IT service provider of the school, or by the IT specialist. A monthly backup will be stored in the safe.

Tablets (School Property)

Eversdal Primary School is in possession of Apple iPads which remain the property of the school at all times. Teachers, who received an iPad for their class, may use it for personal use and may carry it with them wherever they may be.

IPads must be used in the classroom as an additional teaching resource, in a constructive manner, for the teaching of the curriculum.The iPad-trolley must circulate the grade and the last class to use it, on the specific day, must return the trolley to the designated teacher responsible for it. The trolley must be plugged into the charger and the lid left open.

No iPad may be removed from the trolleys without the consent of the IT Department and/or the Headmaster. The school has the right to retract a teacher's iPad and to use/ distribute it as it deems fit.

The school has the right to monitor the use of the iPads for any misuse or unauthorized use, thereof. iPads are monitored from a central computer with the use of approved software, Lightspeed.

The school accepts no responsibility for any data which may be lost on any of the iPads, for whatever reason, whether intentional or not.

Teachers and children are responsible for handling the iPads and iPad case with the necessary care, in order to prevent the possibility of damage occurring.

Teachers connect via 'Eversdal Staff' and the children via the 'BYOD' Wi-Fi connection. Teachers are compelled not to share the password with any learner. Teachers are permitted to download and use their own applications, but must consider the memory of the device, so as not to hamper the functionality of the device by overloading it. The teachers are responsible for remembering the password for their specific device and must keep it safe.

The management of the school has the right to replace any tablets deemed old and not being able to accommodate effective learning. These tablets can be written off, sold or sponsored, whichever accommodates the need of the school.

Cellphones (Non-Learners)

Cellphones may only be used by educators during school hours (07:30 – 14:30) if it is for educational purposes. No other usage is allowed. Personal devices may use the schools' Wi-Fi, with prior consent of the principal. Cellphone usage are prohibited at sport practices. If the educator uses a specific application to the benefit of the sport, it may be permitted.

The use of a cellphone to watch, photograph or store, prohibited pictures, photos or any form of pornography is strongly prohibited by the WCED code of conduct. This applies for the terrain of the school, educational outings or while learners and teachers travel to and from outings and tours.

Access to the worldwide web, email, internet and servers of the school, is filtered and managed by the WCED service provider.

Communication via email on the school network can not been seen as private when used during school hours, school activities, or in the vicinity of the school. This includes any messages, data or media on any devices on the schools network.

BYOD (Bring your own device)

Eversdal Primary gives the opportunity to learners to bring their own devices to school. By doing this, the learner can successfully apply the principles of modern teachers. These devices are the property of the learner, and the parent has to give permission for the learner to participate in the BYOD programme. A learner is only allowed to participate in this programme, once the parent has signed this policy. The school has the right to discontinue a learners' participation if he/she is found to be guilty of misconduct of this policy.

Any learner from grade 4-7 is allowed to bring his/her tablet to school. The conditions are as follow:

- The learners' tablet has to meet the minimum requirements as set out in this policy.
- Tablets with only a Wi-Fi connection is recommended.
- If the tablet does have the 3G/4G function available, no sim-cards are allowed in the device while on school premises or any school related activity.
- The tablet must be connected to the Eversdal "BYOD" Wi-Fi.

The Office365 package must be installed on the tablet. Office products, e.g. One Note, One Drive, Word etc. is a requirement. The learner is allowed to use the tablet for any academic related activities as prescribed by the teacher.

The usage of tablets, on the school premises, during breaks, before and after school is strongly prohibited. Learners with tablets have to put the suitcases in their classroom before school. After school, learner with devices, have to put their suitcases in the designated areas. Aftercare learners have to put their bags in the designated areas in the aftercare. All classrooms, passages and designated areas are monitored by CCTV. The school owns the right to manage the connection of these devices on the network, to ensure effective functionality of the system.

Specific tablet directed lessons for classes will be accommodated by the teacher. During these lessons, the school-owned tablets, will be provided to learners who don't have their own device.

The school doesn't require the parents to load e-books onto the devices. It is optional to all parents. If a parent wants to load e-books onto the device, he/she stays responsible for the cost involved. The tablet and functionality thereof, stays the parents' responsibility.

Accepted Tablets

The following is a list of the minimum specifications and are required to participate in the BYOD programme.

- Any modern tablet with Android 5.0 and higher.
- Apple iOS 10.0 or higher.
- Microsoft Windows 10 or higher.
- 8GB internal storage space
- Unknown makes are not recommended.
- Screen size has to be 7" or bigger.
- A good quality front- and back camera is recommended.
- The tablet must have a long battery life. If the batteries does run flat, the learner can charge his/her device at the designated charging station in the classroom.

These minimum requirements will be updated on a regular basis.

Electronic Projects

Learners use Microsoft products in the daily functioning of the school. This allows easy online storage, which is accessible from home as well. Learners use Onedrive to store their projects. These projects won't be used as formal assessments. Electronic assessments that will be used as assessments, will be managed by the teacher to be completed during the school day.

Cellphones (Learners)

Learners stay responsible for their cellphones. The school, teachers, Education Department or any employee of Eversdal Primary, will not be held responsible or liable for any damage, loss or theft of any cellphone, or any misconduct that the cellphone was used for. Parent will receive this policy and all related arrangements regarding cellphones and it's usage, in the beginning of the new year. Parents have to sign this policy to acknowledge receipt and understanding of this policy and it's contents regarding cellphones.

Learners' cellphones have to switched off during school hours. This applies to breaks as well. If an urgent call needs to be made, it has to be done in the company of a teacher. Cellphones aren't allowed to be seen during school hours.

Cellphones may only be used in the classroom, for academic purposes, under instruction of the teacher. The usage of a cellphone is adjudicated by the teacher, which accepts responsibiltiy for monitoring, control and general usage thereof.

If a cellphone rings, or the learner is caught handling his cellphone, it will be confiscated and locked in the safe for a duration of 5 school days. Parents will be notified by means of a written notice if a learners' phone is confiscated.

The use of a cellphone to watch, photograph or store, prohibited pictures, photos or any form of pornography is strongly prohibited by the WCED code of conduct. This applies for the terrain of the school, educational outings or while learners and teachers travel to and from outings and tours.

Permission to use a cellphone, for reasons other than specified in this policy, may be granted by a teacher if deemed necessary.

Cellphones on camps

Learners should preferably not take cellphones on camps. Most of the time reception is very weak at the camp sites. Learners can go to the teachers to use their phones if a learner needs to speak urgently to his/her parents.

Any learner on a camp, that is found guilty of any misconduct (relating to cellphone usage) as mentioned in this policy, will have his/her phone confiscated immediately for the rest of the camp, outing or tour.

In the case where the whole grade is on a educational camp, the parent will be notified of important information via the school's communication system.

Smart Watches

Eversdal allows the wearing of a smart watch to be used as a watch and for safety purposes. Learners may not use a 3G connection during school hours. This applies to breaks as well. If an urgent call needs to be made, the learner needs to report to reception.

If the smart watch only has a GPS tracking function it will be permitted and not treated as a normal smart watch. These type of watches will be seen as "safety watches".

No external communication is allowed during school hours, this includes break times. Failure to comply with this policy will result in the disciplinenary process to commence.

Ownership and Privacy

In order to manage the safety and welfare of all involved parties, as well as the integrity of the school management systems, the school retains the right to intercept any information, messages, photos or pictures, that is created, received, sent, read on any device, during or at any school represented activity, even if the device is not in use.

It's a condition that permission is given with the signing of this policy to the Eversdal Primary, that the school may investigate any email account, electronic device, as well as social platforms/media, and any user that is suspected of suspicious behavior on any of above mentioned. Reports from eye witnesses may also be investigated.

If it is suspected, within reasonable limits, and according to an eye witnesses report, that any person who is not using his/her cellphone in compliance with this policy, the staff may, under instruction of the principal, examine the information on the cellphone.

If any evidence is found of any misconduct, it has to be reported to the principal. He/she may decide to look further into the matter, by means of a internal disciplinary process, or report it to the Governing Body, School Psychologist, Social Worker, Department of Education or the Police.

Any cellphone that is confiscated may be kept safe for a maximum of five (5) school days. When a cellphone is confiscated, the following information needs to be recorded and documented.

- On which date the phone was confiscated.
- Time that it was confiscated.
- Place where it was confiscated.
- Name of the person who confiscated it.
- Name and adress of the learner from whom it was confiscated.
- Name and adress of the owner of the phone (if it differs from the above).
- Description of the phone, as well as model and series.
- Reason why the phone was confiscated. Supply detail as evidence in the case of appeal.

Acceptance of personal responsibility

Any user of the school's IT systems, will be responsible and accountable to follow the prescribed procedures and to take reasonable steps to protect information dealt with through the system, as well as any other sensitive assets.

The user accepts sole responsibility for all material which is viewed, stored or sent via the school-based computers. The school, however, expects all users to abide by the school rules. Failure to do so may culminate in the suspension or retraction of a user's privileged access, as well as disciplinary steps being taken, including the possibility of civil and/or criminal accountability.

Educators and non-educators who fail to comply with this policy, will be subject to disciplinary proceedings, whether in accordance with the grievance and disciplinary procedures of the school or those of the Department of Basic Education. Learners who do not comply with this policy, will be subject to the school's Code of Conduct for learners.

Policy amendments

The school's Governing Body may from time to time ammend, supplement, adapt or change this policy.

SIGNED ELECTRONICALLY: 2018

MR H.L. ARANGIES
EVERSDAL PRIMARY SCHOOL: HEADMASTER