INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

Date reviewed: 22 July 2020

Date updated: 22 July 2020

Date approved: 25 July 2020

CONTENT

INFORMATION AND COMPUTER TECHNOLOGY

1) INTRODUCTION

This document is the policy for the Information and Computer Technology Systems, as well as the Social Media of **GOLDEN GROVE PRIMARY SCHOOL,** as approved by the Governing Body of the school on date of signature. 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 and 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 intercept any communication that 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 comments 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 that is documented in this policy.

2) TERMINOLOGY

BYOD

Bring Your Own Device. The name of the system that allows learners to bring their own device to the school. This includes tablets, cellphones, etc. **GOLDEN GROVE PRIMARY SCHOOL** is currently in the process of phasing in the BYOD and incorportaing the use of electronic devices in lessons, when needed. Should an educator require an electronic device for a lesson, a request will be sent in writing and timeously via the school communication channels. When not needed, electronic devices are to be handed to the educator at the beginning of the day for safekeeping.

GOLDEN GROVE PRIMARY SCHOOL is not to be held accountable for any possible loss or damage incurred while on the premises, especially if a device was not handed in by the learner.

Information System

The system which consists of all communication channels 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 and exchange information and ideas using virtual community and network platforms. Social media may include text, audio, video, images, podcasting and other communication channels using an internet connection.

System hardware

Any mechanical or electrical apparatus that 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.

3) GENERAL

The school's computer and communication systems are generally for official use only. Nonetheless, occasional personal use is allowed in the instance where no more than a fraction of the number of resources are used that 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 – as well as other – educators, non-educators and learners.

All system hardware and software is the property of **GOLDEN GROVE PRIMARY SCHOOL**. The school is the legal owner of the content of all the files that are stored on its computers and network systems, as well as any messages that are sent by means of these systems. The school reserves the right to access this information without prior consent 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 institution without the prior consent of the Principal.

The school reserves the right to audit the systems from time to time to ensure that this policy is adhered to. The school may, according to its own discretion, 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 remains the individuals' responsibility to conduct backups of his/her personal documents that are stored on his/her computer. The school is not liable for any offensive material that any user may access through the school's system.

Internet Policy

Internet access is available to all **GOLDEN GROVE PRIMARY SCHOOL's** employees where there is a justifiable need.

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 are active to protect the school from improper and indecent material.

The software that 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 indecent and possibly offensive material, will be blocked by means of a 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 ensure compliance to the internet policy, help with internal investigations and assist in the management of the school.

4) E-MAIL POLICY

The school does not guarantee the privacy and confidentiality of any e-mail.
E-mail usage that violates this, or any other policy, is prohibited. Any e-mail content that 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 the school e-mail domain (@ggps.co.za) for commercial purposes is forbidden. Using e-mail with the purpose of abuse, to threaten or offend, is forbidden. E-mail forms part of the management and administrative history of the school and may, therefore, be subject to inspection.

5) HARDWARE

The long-term planning must be evaluated and adjusted annually, with regard to the maintenance and 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 that is replaced, that 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 after permission of the Governing Body is obtained. 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.

6) SOFTWARE

Software programs are installed by the IT Department, ahead of time, according to the needs as determined by management. No illegal and unlicensed software may be installed by the user. Where the user has a need for licensed software for school use, it must be declared to the IT Department. The software must be evaluated and upgraded in order to ensure the system remains relevant. This includes but is not limited to; all operating systems and end-user applications, software updates, antivirus software and updates, etc.

The school issued 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. In the event that software is loaded without consent, and conflicts with the environment, the cost to repair and restore the software environment will be for the user's account.

7) PROHIBITED ACTIVITIES OR BEHAVIOUR

The following activities and/or behaviour are prohibited:

- The copying of material that 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 that 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.

- The use of social media during school hours for personal reasons. This includes, but is not limited to Facebook, Twitter, Instagram or any other social media platform. An exception to the rule would be if these social media platforms are used to promote the school, school functions and events and the various sporting and extra-mural codes.

- The use of the school's information system (included but not limited to electronic devices and networks) for offensive and/or abusive material is prohibited. The following is considered to be computer abuse:

  - Using the school's information system 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 school's information system 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 school's information system to disrupt or cause damage to the academic research, administrative or related endeavours of the school or another person
  - Using the school's information system to violate the academic or any other privacy of a person, or to use it to threaten the person; and
  - Material that is sexist, racist and/or violent or goes against the school's code of conduct.

- The viewing or sending of any material that 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 that 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.

8) CYBER MISCONDUCT

The following forms of cyber misconduct are prohibited:

- Cyber browsing and the misuse of the employers' resources: educators, non-educators and learners may not use the school's resources.

- 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, it is unconstituional and will result in disciplinary proceedings.

- 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 bringing the school's name into disrepute, which may lead to disciplinary or if necessary, 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 that may tarnish the confidentiality of the school.

- 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 that may possibly tarnish the reputation 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 that were taken at official school activities on social media sites. Permission from th eparent / gaurdian will be obtained first. People may be tagged.

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 that could tarnish the name of the school, and a connection to the school is made or is identified or admitted, such person or persons will be subject to disciplinary and, if necessary, legal steps. Legal steps may also be taken against a parent or parents who places the school in disrepute.

All information that 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 on social media must first be approved by the social account administrator. 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 when a learner leaves the school. The school reserves the right to withdraw the privileges and membership of any user at any given time.

Behaviour that 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.

9) SERVER SECURITY

Where possible, all servers that 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 equipped and protected with up-to-date anti-virus software.

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.

GGPS uses the cloud services to backup information. User's information is automatically uploaded and saved on the cloud as soon as an internet connection is established.

10) CCTV

The CCTV system will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice. The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act. Cameras will be used to monitor activities within the school and its grounds to identify criminal activity occurring, anticipated, or perceived. It will be used for securing the safety and wellbeing of the pupils, staff and school together with its visitors.

Materials or knowledge secured because of CCTV will not be used for any commercial purpose. Images will never be released to for the purpose of entertainment. The planning

and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage. Warning signs, as required by the Code of Practice of the Information Commissioner, will be clearly visible on the site.

The CCTV system will be operational 24 hours each day, every day of the year, unless due to unforeseen circumstances that are beyond the control of the school's management.

- The system will be administered and managed by the school's Safety & Security Manager who will act as the Data Controller, in accordance with the principles and objectives expressed in the policy.
- The day-to-day management will be the responsibility of both the Principal and the CCTV System Manager.
- The system and the data collected will only be available to the Data Controller, the Principal and the System Manager.
- Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.
- The System Manager must satisfy themselves of the identity of any person wishing to view images or access the system and the legitimacy of the request. Where any doubt exists, access will be refused.
- Parents may not have access to the footage. The case must be reported to the Head of Discipline and follow the normal disciplinary procedure. The Head of Discipline can request the footage from the Principal who will act accordingly.

The CCTV system in the school can be used for educational purposes with the authority given by the Principal to set up a situation where education can benefit from the footage by way of live viewing.
The CCTV system is to monitor safety and security. It is not to be used as a tool to monitor worker's performance or to spy on someone.

There is a clear difference between live viewing and viewing recordings where the educational need differs from a management or discipline reason.

The following procedure will be followed:

1. The case is reported to the Principal.
2. The Principal informs and provides authorisation to the Data Controller to access the system. A formal document will be signed as proof of the delegated responsibility.
3. The Data Controller will view and download the relevant footage.
4. The footage will be stored in a secure file structure on the network that can only be accessed by the Data Controller, Safety & Security Manager and Principal.

11) CELLPHONES (NON-LEARNERS)

Personal devices may use the schools' Wi-Fi, with prior consent of the Principal.
The use of a cellphone to watch, photograph or store, illicit media content (not limited to images, video, and audio) 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 internet, email, and servers of the school, is filtered and managed by the school's service provider.
Communication via email on the school network cannot be 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.

12) BYOD (Bring Your Own Device)

GOLDEN GROVE PRIMARY SCHOOL currently does not have the necessary policy in place to accommodate for the use of cell phones in class for learning activities. We are in the process of building a working AUP for learners to be able to use this facility freely and safely.

13) ELECTRONIC PROJECTS

Golden Grove Primary is a Microsoft school using the 365 and Teams platform. Each learner will have an email account that will allow access to the online use 365 platform

and the use of the online Office application suite and cloud storage facilities. This account will be active for as long as the learner is enrolled at the school. The policy will take effect upon completion of the setup and activation of the accounts.

14) CELLPHONES (LEARNERS)

Learners are responsible for their cellphones. The cellphones are collected at the beginning of each day and stored in the school safe. The cellphones are collected from the front office at the end of each day and handed back to the learners. At no point is the school, teachers, Education Department, SGB or any employee of **GOLDEN GROVE PRIMARY SCHOOL**, responsible or liable for any damage, loss or theft of any cellphone, or any misconduct that the cellphone was used for. The parent will receive this policy and all related arrangements regarding cellphones and it's usage, at the beginning of the new year. Parents have to sign this policy to acknowledge receipt and understanding of this.

If an urgent call needs to be made, it has to be done in the company of an educator. Cellphones aren't allowed to be visible during school hours, without prior consent from an educator.

If the lesson requires the use of a cellphone, due notice will be sent to the parent in writing, either via a note in the school diary or electronically via class dojo, D6 Communicator or other communication media.
Cellphones may only be used in the classroom, for academic purposes, under the instruction of the educator. The usage of a cellphone is adjudicated by the educator, which accepts responsibility for monitoring, control and general usage thereof.

If a cellphone rings or the learner is caught handling his/her cellphone that goes against the instruction of the educator, it will be confiscated and locked in the safe for a duration of the school day. Parents will be notified by means of written notice if a learners' cellphone 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 educators travel to and from outings and tours.

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

Cellphones on camps

Learners should preferably not take cellphones on camps. Most of the time reception is very weak at the campsites. Learners can go to the educators 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 an educational camp, the parent will be notified of important information via the school's communication system.

Smart Watches

GOLDEN GROVE PRIMARY SCHOOL does not allow the wearing of a smartwatch if it has an activated sim card, or can act as a cellphone when within range of the learner's stored cellphone.
If the smartwatch only has a GPS tracking function, it will be seen as a "safety watch". The school is not responsible for any loss or damage to this device when in possession of the learner.

15) 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 **GOLDEN GROVE PRIMARY SCHOOL**, 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 eyewitnesses may also be investigated.

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 an internal disciplinary process, or report it to the Governing Body, 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 and time the phone was confiscated.
- Reason for confiscation, include where it was confiscated. Supply detail as evidence in the case of appeal.
- Name of the person who confiscated it.
- Name and grade of the learner from whom it was confiscated.
- Name and address of the owner of the phone.
- Description of the phone, as well as model and series.

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 that 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.

16) POLICY AMENDMENTS

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

Signed at: GOLDEN GROVE **on this** 25TH **day of** JULY 2020 **2020**

SGB Chairperson (Mr Ahmed Dalvie)	**School Principal (Ms D Petersen)**

17) PARENT POLICY ACCEPTANCE (To be signed and returned to school)

We,

_____

_____

_____ (print name of parents /legal gaurdian) hereby acknowledge that we have read and accept the content of this Policy. We will ensure that our child / children understand the rules and the consequesnces due, should any transgression occur.

Parent / Legal Gaurdian 1:

Name: _____ (print name)

Sign: _____

Parent / Legal Gaurdian 2:

Name: _____ (print name)

Sign: _____

Date: _____

I, _____ (print learner name)

Learner Sign: _____

Date: _____

I, _____ (print learner name)

Learner Sign: _____

Date: _____