LAERSKOOL NUMBI PRIMARY

Information Systems and Social Media Policy

"We Shape The Future"

"Ons Vorm Die Toekoms"

Table of contents

Policy of the Protection of Personal Information

School Stamp

The SGB adopted this Policy on

2025/10/27

Signatures: _____

SGB Chairperson

_____

School Principal

Information Systems and Social Media Policy

1. Introduction

This document is the information systems and social media policy of Laerskool Numbi, as approved by the school governing body on 27th of October 2025. The policy has been drafted in accordance with the provisions of the Constitution of South Africa, 1996; the South African Schools Act 84 of 1996 ('SASA'); the National Education Policy Act 27 of 1996; applicable provincial legislation on school education, and the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

The purpose of this policy is to govern the use of the school's information systems for the conveyance of communication-related information and the appropriate use of social media platforms by educators, non-educators, and learners. The school recognises the evolution of social media as a mode of communication, but also realises that to optimise its use, it must be used responsibly.

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

In terms of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002, "any person may intercept any communication if he or she is a party to the communication, unless such person intercepts such communication for purposes of committing an offence". The school may therefore intercept any communication transmitted through its information systems or social media platforms that refers to the school.

2. Philosophy

The school is committed to the highest standards of conduct and ethics, and its success is built on integrity in all school matters. The school recognises that emerging online collaboration is changing the way individuals and organisations communicate, and that social media platforms are a large part of people's lives during and after school hours. Therefore, the school encourages ethical and responsible engagement on all social media platforms.

3. Application

This policy applies to all users of the school's information and information systems. It also applies to the expression of opinions and comments by educators, non-educators and learners on social media that may in any manner be linked to the school.

4. Definitions

Information systems – the systems consisting of the network of all communication channels used within the school.

Intercept – the aural or other acquisition of the contents of any communication by any means to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient thereof, and includes the —

(a) monitoring of any such communication by means of a monitoring device;

(b) viewing, examination or inspection of the contents of any indirect communication; and

(c) diversion of any indirect communication from its intended destination to any other destination.

IT – information technology.

School – the school governing body, as well as any person to whom particular authority or functions have been delegated in terms of this policy.

School management – the principal or a member of the school staff delegated by the principal.

Social media – the means of interaction among people during which they create, share and exchange information and ideas in virtual communities and networks. Social media can include, but is not limited to, text, audio, video, images, podcasts, blogs, wikis, photo-sharing (including YouTube, Flickr, and Instagram), and online social networks such as Facebook, Twitter, LinkedIn, Google+, Myspace, and any other multimedia communications.

Social media platforms – blogs, micro-blogs, wikis, social networks, social bookmarking services, user rating services and any other online collaboration, sharing or publishing platform, whether accessed via the web, a mobile device, text messaging or any other existing and/or future communication medium.

Systems hardware – any mechanical or electronic device linked to a computer system, including the central processing unit and added or additional devices such as printers and external disk drives.

Systems software – computer software designed to operate and control the computer hardware and to provide a platform for running application software.

5. General

5.1. In general, the school's computer and communication systems are intended for official school purposes only. Incidental personal use is nonetheless permissible if the use does not consume more than a trivial amount of resources that could have otherwise been used for official purposes; does not interfere with worker productivity; does not detract from any school activity, and does not cause distress, legal problems or morale problems for the school or other educators, non-educators and learners.

5.2. All systems, hardware, and software are the property of (school's name). The school has legal ownership of the contents of all files stored on its computer and network systems, as well as all messages transmitted via these systems. The school reserves the right to access this information without prior notice whenever a genuine business need exists.

5.3. The school reserves the right to audit systems periodically to ensure compliance with this policy.

5.4. The school may, at its own discretion, examine, move or delete files, including electronic mail (e-mail), for purposes of system maintenance or if the files are determined to be disruptive to the system or its users, either intentionally or unintentionally.

5.5. The school provides no warranties of any kind, whether expressed or implied, for the services it offers.

5.6. The school will not be responsible for any damages suffered while on this system, including loss of personal data due to system outages or irresponsible use.

5.7. The school is not responsible for offensive material obtained by any user using the school's information systems.

6. Internet Policy

6.1. Internet access shall be granted to employees who have a legitimate need for such access, for which the user needs to apply formally. All internet connections shall be via the school's approved internet service provider. Any other connections are prohibited.

6.2. Internet use is a privilege, which constitutes the acceptance of responsibilities and obligations that are subject to government policies and laws. Acceptable use must be legal, ethical, and respectful of intellectual property, data ownership, system security mechanisms, and individual rights to privacy and freedom from intimidation, harassment, and annoyance.

6.3. Users shall be subject to limitations on their internet use, as determined by the appropriate supervising authority.

6.4. To protect the school from profane material and to minimise the use of bandwidth, all internet use shall be monitored by web content filtering software.

6.5. Content filtering software shall prevent users from connecting to certain websites that do not relate to school business. All websites that contain sexually explicit, profane and other potentially offensive material shall be blocked via the proxy server.

6.6. At any time and without prior notice, school management reserves the right to examine web browser cache files, web browser bookmarks and other information that are stored on or passing through the computers of the school. Such management access ensures compliance with internal policies, supports internal investigations, and helps manage the school.

7. **E-mail policy**

7.1. The school does not guarantee privacy or confidentiality of any e-mail.

7.2. Use of e-mail to violate this or any school policy is prohibited.

7.3. Any use of e-mail that does not reflect the image and reputation of the school is prohibited.

7.4. The user bears sole responsibility for all transmissions using their assigned e-mail address.

7.5. Concealment or misrepresentation of names, addresses, or affiliations in e-mail is prohibited.

7.6. Use of e-mail for commercial purposes is prohibited.

7.7. Use of e-mail that is threatening, offensive or intended for purposes of harassment is prohibited.

7.8. E-mail is part of the business or administration record of the school, and may be inspected.

8. **Prohibited activities or behaviour**

The following activities and/or behaviour are prohibited:

8.1. Copying material bearing copyrights or patents, without proper licensing or authority

8.2. Using the school's information systems for political lobbying, personal gain or commercial purposes

8.3. Copying or removing software from the school's computers

8.4. Downloading material from the internet that is not related to official school activities or business

8.5. Installation of system hardware or software by unauthorised personnel. Under no circumstances shall unlicensed software, privately owned software, games, public-domain software, and freeware, shareware or demonstration software be loaded onto official computer equipment without prior written consent from the governing body.

8.6. Using the school's information system for offensive or harassing material. The following shall constitute computer harassment: (1) using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures or other materials, or threats of bodily or psychological harm to the recipient; (2) using the computer to contact another person repeatedly with the intent to annoy, harass or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) using the computer to contact another person repeatedly regarding a matter about which one does not have the legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease; (4) using the computer to disrupt or damage the academic research, administrative or related pursuits of the school or another person; (5) using the computer to invade the privacy, academic or otherwise, of another, or the threatened invasion of privacy of another; and (6) material containing sexist, racist and/or violent content.

8.7. Using the school's information system for discriminatory material. Users must have respect for all persons and avoid discriminatory behaviour and the victimisation of other social media users, whether based on gender, race, class, creed, colour, sexual orientation, marital or family status, age, nationality, political belief, religion, or disability.

8.8. Viewing or transmission of any material that violates any national, provincial or international law

8.9. Use of school information systems to gain unauthorised access to any system or data

8.10. Accessing, downloading, storing or transmitting obscene material through the school's computer network system

Each educator and non-educator shall be granted access to information as needed to perform their assigned functions. Still, they shall not be given access to information that would otherwise require

protection unless and until such access is necessary and formally authorised. Authorised users are responsible for the security of their passwords and accounts.

The following acts of 'cyber-misconduct' are prohibited:

8.11. 'Cyber-loafing' and the abuse of the employer's resources: Educators, non-educators and learners are prohibited from using the school's resources, e.g. computers, telephones, etc., for private purposes during or outside school time, thereby abusing the employment relationship.

8.12. Creating disharmony and distributing offensive or abusive material: Educators, non-educators and learners may not circulate information that is racist, defamatory, sexist or pornographic. This constitutes gross misconduct. Racist comments are not only offensive but also create disharmony among people.

8.13. Derogatory statements: Educators, non-educators, and learners may not post or distribute derogatory or offensive messages about the school, its staff, or learners. An offender may be found guilty of bringing the school into disrepute, which could lead to disciplinary action or legal action for defamation.

8.14. Breach of trust: Educators, non-educators and learners may not use the school's information, information systems or social media platforms in a way that breaches the school's trust.

9. Engaging in social media communication on behalf of the school

9.1. Only persons who are authorised by the school governing body ("authorised persons") may engage in social media communication on behalf of the school.

9.2. Only authorised persons may comment on any aspect of the school and/or any matter in which the school is involved. When making such a comment, the authorised person must identify themself.

9.3. An authorised person who engages in social media communication on behalf of the school must ensure that they are familiar with the school's view on specific issues, and should not express opinions that are inconsistent with those set out by the school.

9.4. If an authorised person is not familiar with or is unsure of the school's position on any particular issue, they should seek clarity from the school governing body.

9.5. The school may instruct authorised persons to avoid specific subjects/topics, and has the right to monitor and review authorised persons' comments and submissions. The school shall take appropriate action against any authorised person who makes comments or submissions that the school has not authorised.

10. **Educators, non-educators, learners, and parents using social media for official and non-official purposes should be aware of the following:**

10.1. The approved social media sites may only be used for official purposes when using the school's information systems.

10.2. The message that the school wants to convey to other users must be clearly defined.

10.3. Postings must be kept legal, ethical and respectful.

10.4. Educators, non-educators and learners may not engage in online communication activities that could bring the school into disrepute, and have a responsibility to avoid establishing online relationships and/or interests that could adversely influence or impair their capacity to act with integrity and objectivity in relation to the school as well as other educators, non-educators and learners. In addition, they should refrain from engaging in any social media activities that may bring the school into disrepute, and they will be held accountable for any such behaviour.

10.5. Personal details of educators, non-educators, learners and parents may not be disclosed. Educators, non-educators, learners, and parents should note that the school may, from time to time, share photos on social media sites taken during official school activities. People may then be 'tagged'. Users of these social media sites are advised to check their security settings if they prefer to review postings in which they were 'tagged'. Educators, non-educators and learners are advised to block other users whom they do not know or do not want to be associated with from accessing their profiles.

10.6. The school does not accept any responsibility or liability for weak security settings on the social media profile of any person associated with the school.

10.7. If any educator, non-educator, learner or parent posts a remark, photo or video on any social media platform that may harm the reputation of the school, and affiliation to the school is identified, known or presumed, such educator, non-educator, learner, or parent will be subject to disciplinary and legal action. Legal action may be taken against a parent who jeopardises the school's reputation.

10.8. All information that is published must be accurate, and confidential information may not be disclosed.

10.9. Copyright laws must be adhered to.

10.10. Only the officially approved logo of the school may be used when participating in social media communication on behalf of the school.

10.11. The governing body must first approve statements to the media.

10.12. All school information systems privileges shall be promptly terminated when an educator or non-educator ceases to provide services to the school, or when a learner leaves the school. The school reserves the right to revoke any user's privileges at any time.

10.13. Conduct that interferes with the regular and proper operation of information systems, adversely affects the ability of others to use these information systems, or is harmful or offensive to others shall not be permitted

11. CCTV Surveillance Policy

11.1. Purpose

11.1.1. This policy regulates the management and use of closed-circuit television (CCTV) systems at the school.

11.1.2. The system is intended to enhance the safety and security of staff, learners, visitors, and property, while ensuring compliance with the Protection of Personal Information Act (POPIA), 2013.

11.2. Scope

11.2.1. This policy applies to all CCTV cameras installed within the school premises, including:

11.2.1.1. Phase 1: Office block (internal and external areas)

11.2.1.2. Phase 2: Classrooms and corridors

11.2.1.3. Phase 3: Sports field, bottom parking area, and multipurpose centre

11.2.2. It applies to all staff, learners, contractors, parents, and visitors entering the school premises.

11.3. Objectives

11.3.1. To enhance the safety and security of learners, staff, and visitors.

11.3.2. To protect school assets against theft, vandalism, and damage.

11.3.3. To support disciplinary or legal investigations when necessary.

11.3.4. To ensure compliance with POPIA and related laws.

11.4. System Overview

11.4.1. CCTV cameras record both audio and visual footage.

11.4.2. Footage is stored securely and retained for a maximum of three (3) weeks, after which it is automatically overwritten, unless required for an ongoing investigation.

11.4.3. Cameras operate continuously, 24 hours a day.

11.4.4. Clear signage has been installed at strategic entry points and common areas to inform staff, learners, and visitors of surveillance activity.

11.4.5. Visitors who do not wish to be recorded may choose not to enter the premises upon notification at the school gate.

11.5. Consent

11.5.1. Teacher Consent: All teaching and non-teaching staff have provided consent for the use of CCTV within school premises.

11.5.2. Parent Consent: The school will not request consent from parents, as the installation of cameras serves a legitimate safety and operational purpose within the school environment. The purpose is to ensure protection, discipline, and effective management—not to collect personal information beyond what is necessary for these functions.

11.5.3. This approach is consistent with the "legitimate interest" and "safety and security" provisions under POPIA.

11.6. Use of Recorded Material

11.6.1. CCTV recordings may only be used for safety, security, disciplinary, or legal purposes.

11.6.2. Recordings may not be used for personal, discriminatory, or non-official purposes.

11.6.3. Meetings held in the boardroom must begin with the chairperson informing attendees that the session is being recorded (audio and video).

11.7. Access to Footage

11.7.1. Only authorised personnel (Principal, ICT Chairperson, or Information Officer and deputy information officer) may access CCTV footage.

11.7.2. Requests to view or obtain a copy of any footage must be submitted in writing to the Information Officer.

11.7.3. The Information Officer will determine whether access is lawful, proportionate, and consistent with POPIA.

11.7.4. Any approved disclosure must be recorded in an access log.

11.8. Data Protection and POPIA Compliance

11.8.1. The school commits to protecting personal information collected through CCTV in line with POPIA:

11.8.1.1. Processing will be lawful, fair, and transparent.

11.8.1.2. Data will be used solely for explicit and legitimate purposes.

11.8.1.3. Access will be restricted to authorised staff only.

11.8.1.4. Appropriate technical and physical safeguards are in place to prevent misuse, alteration, or unauthorised disclosure.

11.8.1.5. Individuals may request confirmation of whether their personal information is held and may request access through the Information Officer, subject to legal restrictions.

11.8.1.6. Any breach involving CCTV data must be immediately reported to the Information Officer and handled in accordance with the school's data breach procedures.

11.9. Retention and Disposal

11.9.1. CCTV recordings are retained for up to three (3) weeks.

11.9.2. After this period, footage is automatically deleted or overwritten unless required for an official investigation.

11.9.3. Copies extracted for investigations will be securely stored and destroyed once the matter concludes.

11.10. Responsibilities

11.10.1. Information Officer: Oversees compliance with POPIA and this policy.

11.10.2. ICT Chairperson: Maintains secure systems and technical infrastructure.

11.10.3. Principal: Authorises disclosure and ensures responsible use of surveillance data.

11.11. Breach of Policy

11.11.1. Unauthorised access, use, or disclosure of CCTV footage constitutes misconduct and may lead to disciplinary action and/or legal consequences under POPIA.

11.12. Review

11.12.1. This policy will be reviewed annually or upon completion of each project phase to ensure its ongoing effectiveness and compliance with legal standards.

12. **Server security**

12.1. Where feasible, all servers hosting data and applications shall be located in a physically secure environment where access is strictly controlled. All server rooms shall be considered high-risk security areas, with access strictly controlled.

12.2. All servers shall be loaded and protected with the latest, approved anti-virus software. Updates for patches and upgrades shall be implemented regularly by the designated IT service provider or, when required, by the school's IT specialist.

12.3. Only an authorised administrator shall be granted administrative rights to the servers. Administrative passwords shall be kept secret, and only personnel nominated by the school shall have access to them.

12.4. All business or administrative critical data on local computer and notebook hard drives must be copied or moved to a “My Documents” share on a file server, where it will be backed up. Where such an action is not possible, for example, due to being away from the school network, the data must be copied over at the first available opportunity. It will be the sole responsibility of the user to back up and maintain data security at all times.

12.5. Servers shall be backed up every month by the IT service provider or the school’s IT specialist

13. Acceptance of personal responsibility

Any person who uses a school's information system shall be responsible and accountable for following recommended procedures and for taking all reasonable steps to safeguard the information handled by that system, as well as any sensitive assets involved. The user is solely responsible for all materials viewed, stored or transmitted from school-based computers. However, the school expects users to comply with all school rules. Failure to do so may result in the suspension or revocation of a user’s access privileges as well as disciplinary measures, including the possibility of civil and/or criminal liability. Educators and non-educators who fail to adhere to this policy will be subject to disciplinary proceedings under either the school's grievance and disciplinary procedure or procedures conducted by the Department of Basic Education. Learners who fail to comply with this policy will be subject to the school’s code of conduct for learners.

14. Policy amendments

The school governing body may amend, supplement, modify or alter this policy from time to time.