ELECTRONIC COMMUNICATION AND NETWORK USAGE POLICY

APPLICABILITY

Applies to all "Ethembeni Enrichment Centre" students, staff, and all others using computer and communication technologies, including the school's network, whether personally or school owned, which access, transmit or store The Settlers High School or pupil information.

POLICY STATEMENT

Use of Ethembeni Enrichment Centre network and computer resources should support the basic missions of the school in teaching, learning and research. Users of school's network and computer resources ("users") are responsible to properly use and protect information resources and to respect the rights of others. This policy provides guidelines for the appropriate use of information resources.

SUMMARY

This policy covers the appropriate use of all information resources including computers, networks, and the information contained therein.

Section headings are:

1. POLICY SCOPE AND APPLICABILITY

2. POLICIES

3. OVERSIGHT OF INFORMATION RESOURCES

4. REPORTING AND INVESTIGATING VIOLATIONS OR SCHOOL CONCERNS

5. CONSEQUENCES OF MISUSE OF COMPUTING PRIVILEGES

6. COGNIZANT OFFICE

7. RELATED POLICIES

1. DEFINITIONS

As used in this policy:

a. "Information resources" are all computer and communication devices and other technologies which access, store or transmit school or pupil information.

b. “Information” includes both school, staff and pupil information.

2. POLICIES

a. General Policy -- Users of school information resources must protect:

(i) their online identity from use by another individual,

(ii) the integrity of computer-based information resources, and

(iii) the privacy of electronic information.

In addition, users must refrain from seeking to gain unauthorized access, honour all copyrights and licenses and respect the rights of other information resources.

b. Access

Users must refrain from seeking to gain unauthorized access to information resources or enabling unauthorized access. Attempts to gain unauthorized access to a system or to another person’s information are a violation of school policy and may also violate applicable laws, potentially subjecting the user to both civil and criminal liability. However, authorized system administrators may access information resources, but only for a legitimate operational purpose and only the minimum access required to accomplish this legitimate operational purpose.

1. Prohibition against Sharing User IDs and Passwords -- Sharing an online identity (user ID and/or password) violates school policy.

2. Information Belonging to Others—Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or other digital materials belonging to other users, without the specific permission of those other users.

3. Abuse of Computing Privileges — Users of school information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the school. For example, abuse of external networks to which the school belongs or the computers at other physical sites connected to those networks will be treated as an abuse of school computing privileges.

c. Usage

The school is a non-profit, tax-exempt organization and, as such, is subject to specific national, provincial and local laws regarding sources of income, political activities, use of property and similar matters. It also is a contractor with government and other entities and thus must assure proper use of property under its control and allocation of overhead and similar costs. Use of the school’s information resources must comply with school policies and legal obligations (including licenses and contracts), and all national and provincial laws.

1. **Prohibited Use** — Users must not send, view or download fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of applicable law or

school policy. In particular, contributing to the creation of a hostile academic or work environment is prohibited.

2. **Copyrights and Licenses** —Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file-sharing using the school's information resources is a violation of this policy.

3. **Social Media**—Users must respect the purpose of and abide by the terms of use of online media forums, including social networking websites, mailing lists, chat rooms and blogs.

4. **Political Use** — school information resources must not be used for partisan political activities.

5. **Personal Use** — school information resources should not be used for activities unrelated to appropriate school functions, except in a purely incidental manner.

6. **Commercial Use** — school information resources should not be used for commercial purposes, including advertisements, solicitations, promotions or other commercial messages, except as permitted under school policy. Any such permitted commercial use should be properly related to school activities, take into account proper cost allocations for government and other overhead determinations, and provide for appropriate reimbursement to the school for taxes and other costs the school may incur by reason of the commercial use. The HEADMASTER and HEAD OF THE INFORMATION MANAGEMENT COMMITTEE will determine permitted commercial uses.

7. Use of school information resources — Users must abide by applicable data storage and transmission policies

d. Integrity of Information Resources

Users must respect the integrity of information and information resources.

1. **Modification or Removal of Information or Information Resources** — Unless they have proper authorization, users must not attempt to modify or remove information or information resources that are owned or used by others.

2. **Other Prohibited Activities** — Users must not encroach on, disrupt or otherwise interfere with access or use of the school's information or information resources. (Hacking) For the avoidance of doubt, without express permission, users must not give away school information or send bulk unsolicited email. In addition, users must not engage in other activities that damage, vandalize or otherwise compromise the integrity of school information or information resources.

3. **Academic Pursuits** — The school recognizes the value of legitimate research projects undertaken by staff and pupils under subject field supervision. The school may restrict such activities in order to protect school and individual information and information resources, but in doing so will take into account legitimate academic pursuits.

e. Locally Defined and External Conditions of Use

Individual units within the school may define "conditions of use" for information resources under their control.

These statements must be consistent with this overall policy but may provide additional detail, guidelines restrictions, and/or enforcement mechanisms. Where such conditions of use exist, the individual units are responsible for publicizing and enforcing both the conditions of use and this policy. Where use of external networks is involved, policies governing such use also are applicable and must be followed.

f. **Access for Legal and School Processes**

Under some circumstances, as a result of investigations, subpoenas or lawsuits, the school may be required by law to provide electronic or other records, or information related to those records or relating to use of information resources, ("information records") to third parties. Additionally, the school may in its reasonable discretion review information records, e.g., for the proper functioning of the school, in connection with investigations, or to protect the safety of individuals or the Settlers community. The school may also permit reasonable access to data to third-party service providers in order to provide, maintain or improve services to the school. Accordingly, users of school information resources do not have a reasonable expectation of privacy when using the school's information resources.

3. **OVERSIGHT OF INFORMATION RESOURCES**

Responsibility for, and management and operation of, information resources is delegated to the head of a specific subdivision of the school governance structure ("department and subject head"). This person will be responsible for compliance with all school policies relating to the use of information resources owned, used or otherwise residing in their department. The subject head/department head may designate another person to manage and operate the system, but responsibility for information resources remains with the subject head/department head.
The Head of the Information Management Committee is responsible for managing and operating information resources under their oversight in compliance with school and department policies, including accessing information resources necessary to maintain operation of the systems under the care of the system administrator.

a. **Responsibilities** — The system administrator/ IT coordinator should:

• Take all appropriate actions to protect the security of information and information resources.

• Take precautions against theft of or damage to information resources.

• Faithfully execute all licensing agreements applicable to information resources.

• Communicate this policy, and other applicable information use, security and privacy policies and procedures to their information resource users.

b. **Suspension of Privileges** — System administrators may temporarily suspend access to information resources if they believe it is necessary or appropriate to maintain the integrity of the information resources under their oversight.

4. **REPORTING AND INVESTIGATING VIOLATIONS OR CONCERNS**

a. **Reporting Violations** — System users will report violations of this policy to the Information Manco Head, and will immediately report defects in system accounting, concerns with system security, or suspected unlawful or improper system activities to the Information Manco Head during normal business hours.

b. Accessing Information & Systems– Inspecting and monitoring information and information resources may be required for the purposes of enforcing this policy, conducting school investigations, ensuring the safety of an individual or the settlers community, complying with law or ensuring proper operation of information resources. Only the school's Information Manco Head (or designate) may authorize this inspection and monitoring.

c. Cooperation Expected — Information resource users are expected to cooperate with any investigation of policy abuse. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions.

5. **CONSEQUENCES OF MISUSE OF INFORMATION RESOURCES**

A user found to have violated this policy may also have violated The Ethembeni Enrichment Centre's Code of Conduct, the Ethics Code, and/or other school policies, and will be subject to appropriate disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action. The Information Manco Head will refer violations to the Deputy Principal, the Principal, and for other teaching or research personnel, if appropriate.

6. **COGNIZANT OFFICE**

The Ethembeni Enrichement Centre's Information Manco Head, or other person designated by the Headmaster, shall be the primary contact for the interpretation, monitoring and enforcement of this policy.

7. **RELATED POLICIES**

a. **Pupil Discipline** : Codes of Conduct and Ethics

b. **Staff Discipline**: Codes of Conduct and Ethics and Employment Contracts (Governing Body and ECED)

c. **Patents and Copyrights** — general South African Laws passed by national and provincial parliaments.

d. **Partisan Political Activities** — ECED policies

e. **Ownership of Documents**— copyright laws (national and international documents)

f. **Security of Information** -- Access to Information Act.

SPECIAL LIMITATIONS:

1. All users must LOG OFF properly at the end of a session. Should a user's account details be used by a third party, he/she will be liable!

2. Staff are not allowed to download any non- educational music or movies etc. on the school's bandwidth.

3. Private printing should not be done in the Staff workroom

4. No social media may be registered on school e-mail accounts.

5. All electronic communications from the school must be BRANDING COMPLIANT.

6. Pupils and staff may not treat school equipment as their own by changing backgrounds, wallpapers etc.

7. Departments, teachers and pupils will be held severally liable for breakages. (This does not apply to fair wear and tear)

8. When physical ports are available, WiFi should not be used.

9. No pupil may use Facebook, Twitter or any other social media on the school's equipment and bandwidth.

10. The IT Co-ordinator/System Administrator needs to be informed of tablets / cellphones used on the school's WiFi system.

SIGNED ON:_____

SGB CHAIRPERSON:_____

PRINCIPAL: _____

TREASURER:_____

SECRETARY:_____