BELLEVUE
SCHOOL
NAIROBI, KENYA

Internet Access Policy

Policy Number:	IA - 2025 - 001	Version:	1.0
Approval Date:	01-AUG-2025	Approved By:	Charity Kamau
Effective Date:	01-AUG-2025	Next Review Date:	01-AUG-2026
Title:	Principal	Department:	Academic Affairs

Purpose / Objective

Explains why the policy exists and the problem it addresses or goal it aims to achieve.

This Internet Access Policy exists to ensure that the school's internet resources are used safely, responsibly, and for educational purposes. The policy addresses growing concerns about online safety, digital distractions, and the misuse of school technology.

The goals of this policy are to:

- Promote safe and purposeful use of the internet in support of teaching, learning, and school operations.
- Protect students and staff from exposure to harmful or inappropriate content, cyberbullying, and online exploitation.
- Establish clear expectations around digital behavior and internet use within school premises.
- Safeguard the integrity and security of the school's digital infrastructure and network.
- Support digital literacy by encouraging responsible online citizenship and information evaluation

Scope

Defines who the policy applies to (e.g., staff, students, parents) and when or where it applies.

This policy applies to all members of the school community who access the internet using school-provided devices, school Wi-Fi networks, or while on school premises. This includes:

- Students – regardless of age or ability.
- Teaching and Non-Teaching Staff – including administrators, support staff, and temporary or volunteer personnel.
- Parents and Visitors – when granted internet access through the school's guest network or while using school devices.

The policy applies in the following contexts:

- During school hours and any school-related activities on or off campus
- When using school-owned devices (e.g., laptops, tablets, smartboards).
- When connected to the school's internet or Wi-Fi network, even on personal devices.
- When engaging in school-related digital communication, including emails, virtual learning platforms, or school-approved apps.

Policy Statement

The core rules or principles of the policy. Outlines what is allowed, required, or prohibited.

The following rules govern the acceptable and responsible use of the internet within the school environment:

1. **Educational Use Only**
   Internet access must be used for learning and school-related work only.
2. **Respectful Online Behavior**
   All users must be respectful online. Cyberbullying, offensive language, impersonation, and spreading false information are not allowed.
3. **Banned Content and Activities**
   Viewing or sharing violent, pornographic, or illegal content is prohibited. Users must not bypass filters, use VPNs, or engage in hacking.
4. **Privacy and Security**
   Do not share passwords or access other people's accounts. Do not damage school devices or systems, and keep personal information private.
5. **Supervised Student Use**
   Students must use the internet under staff supervision. Younger students should be guided when going online.

6. **Personal Devices**
   Personal devices may only connect to school networks with permission and must be used only during approved times.

5. Definitions

Explains key terms used in the policy to ensure clarity and avoid misinterpretation.

To avoid misinterpretation, the following terms are defined as used in this policy:

1. **Acceptable Use:** Use of the internet that supports learning, follows school rules, and complies with legal and ethical standards.
2. **Inappropriate Content:** Online material that is violent, pornographic, hateful, illegal, or otherwise unsuitable for a school environment.
3. **Cyberbullying:** Using digital platforms to harass, threaten, or harm others.
4. **Personal Device:** Any privately owned device (e.g., phone, tablet, laptop) used to access the internet at school.
5. **Plagiarism:** Copying someone else's online content or ideas and presenting them as your own.
6. **VPN (Virtual Private Network):** A tool used to bypass internet restrictions; not allowed on school networks.

Roles and Responsibilities

Specifies who is responsible for implementing, enforcing, or reviewing the policy.

Role	Responsibilities
School Principal / Headteacher	- Oversees overall enforcement of the policy- Ensures all stakeholders are informed- Authorizes disciplinary actions for major violations
ICT Coordinator / IT Manager	- Maintains secure network access and filtering systems- Monitors internet usage and investigates misuse- Supports digital safety training
Teachers and Staff	- Supervise student internet use during lessons- Report any misuse or safety concerns- Model appropriate digital behavior

Students	- Use the internet responsibly and for educational purposes only- Follow all rules outlined in this policy- Report any unsafe or inappropriate content
Parents and Guardians	- Reinforce safe internet use at home- Support school efforts in promoting responsible online behavior
School Board	- Reviews and approves policy updates- Supports accountability and alignment with legal or curriculum standards
Digital Safety Committee (if applicable)	- Reviews incidents and advises on improvements- Evaluates digital risks and updates policy recommendations periodically

Procedures / Implementation Guidelines

Step-by-step instructions for how the policy will be put into practice.

To ensure effective use of this policy, the following step-by-step actions will be taken:

1. **Policy Approval and Communication**

The policy is approved by school leadership or the governing body. It is shared with staff, students, and parents via the school website, handbooks, meetings, and student orientation sessions.

2. **Training and Awareness**

Staff are trained annually on safe internet use, monitoring, and incident response. Students are oriented on acceptable use, digital safety, and consequences of misuse. Parents receive resources to support safe internet use at home.

3. **Access Control and Supervision**

School internet is secured with filters, firewalls, and role-based access.Supervision is provided in classrooms and labs. IT staff monitor network activity and flag unusual behavior.

4. **Handling Violations**

Reports of misuse are handled by relevant staff. Consequences range from warnings to restricted access or disciplinary action. Serious cases (e.g., cyberbullying or illegal activity) are escalated appropriately.

5. **Ongoing Review**

The policy is reviewed annually or biennially based on emerging risks, tech changes, and feedback from the school community.

Compliance and Enforcement

Outlines how adherence will be monitored and what happens in case of non-compliance.

Failure to comply with the Internet Access Policy will result in appropriate disciplinary or corrective action, depending on the severity and frequency of the violation.

For Students

1. First Offense: Verbal warning and guidance; possible short-term restriction of device or internet access.
2. Repeated or Serious Violations: Written warning, parent notification, and suspension of access to digital resources; disciplinary action may follow.
3. Severe Misconduct (e.g., harmful content, cyberbullying, hacking): Immediate loss of privileges, referral to administration or child protection, and possible law enforcement involvement.

For Staff

- Unintentional Breach: Policy reminder, retraining if needed, and incident logged.
- Negligent or Willful Breach: Formal warning, possible access restriction, investigation, and disciplinary action per staff code—up to suspension or dismissal.

Related Documents / References

Lists other policies, laws, or documents that relate to or support the policy.

- Kenya Basic Education Act
- Children's Act (Kenya)
- Teachers Service Commission (TSC) Code of Conduct and Ethics
- Relevant Ministry of Education Guidelines
