E.S.I

EDUCATIONAL STYLED INTEGRATION

CYBER SAFETY POLICY

2021

Important terms used in this document

- The abbreviation ICT in this document refers to the term “Information and Communications Technology”
- “Cyber Safety” refers to the safe and responsible use of the internet and ICT equipment/devices, including cellular phones.
- The ICT equipment/devices used in this document includes but is not limited to, computers, (such as desktops, laptops, Ipads), storage device (such as USB and flash memory devices, CD’s, DVD,sIpods, MP3 players, cameras, video recorders, digital webcams) all types of mobile phones, videos, audio players/receivers (such as portable CD and DVD players), gaming consoles and any other similar technology as they come into use.

1. Cyber Safety Policy

ESI has a statutory obligation to maintain a safe physical and emotional environment.

These responsibilities are increasingly being influenced by the use of the internet and ICT, and a number of related cyber safety issues. The Internet and ICT devices and equipment bring great benefits to the teaching and learning programmes and to the effective operation of the school.

The school however also recognises that the presence in the learning environment of these technologies (some provided partly or wholly by the school and some privately owned by staff, students and other members of the school community), can also facilitate anti-social, inappropriate and even illegal material and activities.

The school has the dual responsibility to maximise the benefits of these technologies, while at the same time to minimise and manage the risks.

The school thus acknowledges the need to have in place rigorous and effective school cyber safety practices which are directed and guided by this Cyber Safety Policy.

The cyber safety practices that are presented, will aim to not only maintain a cyber safe environment, but also aim to address the need of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication.

To develop a cyber safe school environment, the School will delegate to the Principal the responsibility to achieve this goal by developing and implementing the appropriate management procedures, practices, electronic systems and educational programmes. These will be based and fall within the ambits of relevant legislation.

2. Practices in this Cyber Safety Policy.

2.1 The school's Cyber Safety practices are based on relevant legislation within the Republic of South Africa.

2.2 All persons using the school internet facilities and school owned/leased ICT devices/equipment and software are in all circumstances subjected to the policy of the school. This policy also applies to the use of privately owned/leased devices/equipment on the school site, or at/for any school related activity, regardless of its location. This includes Off-site access to the school's network from school or privately owned/leased devices/equipment.

2.3 This policy covers all school employees (fulltime, part time or on contract), all students and any other individual authorised to make use of the school internet facilitates and ICT devices/equipment and software..

2.4 The policy is also an educational tool and should be used as a resource to the professional development of staff and students.

2.5 Use of the Internet and ICT devices/equipment and school software by staff, students and other approved users at ESI is to be limited to educational, professional development and personal usage appropriate in the school environment.

2.6 The school has the right to monitor access and review all use. This includes all emails sent and received on the schools computers and /or network facilities at all times.

2.7 The school has the right to audit any material, equipment and software that is owned/leased by the school. The school may also request permission to audit privately owned ICT equipment used on the school premises or at or for any school related activity.

2.8 Issues relating to confidentiality, such as sighting student or staff information, reason for collecting data and the secure storage of personal details and information (including images) will be subject to any legislation that falls within the constitution of South Africa (Act 108 of 1996).

2.9 The safety of children is of paramount concern. Any apparent breach of cyber safety will be taken seriously. The response to individual incidents will follow normal school investigative procedure. Specific attention will be paid to the need for gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the South African police or School Board.

Parents are required to support their children carrying out the requirements of the policy.

3. Information and Communications Technologies Policy for members of Staff.

3.1 ESI believes in a model for supporting safe and responsible use of the internet in a teaching and learning context. A vital part of fostering this culture is the support that is provided to students by “role model educators” around them. One of the most important parts of this guidance is the modelling of good digital cyber skills that young people observe in their day to day interactions. ESI defines a successful digital cyber individual as a staff member who:

- Is a confident and capable user of ICT
- Use technology in educational, cultural and economic activities.
- Uses and develops critical thinking skills in cyberspace.
- Is literate in language, symbols and texts of digital technologies.
- Is aware of ICT challenges and can manage them effectively.
- Demonstrates honesty and integrity in their use of ICT.

□

- Respects the concepts of privacy and freedom of speech in a digital world. Contributes and actively promotes the values of digital use.

3.2 Guidelines for responsible use.

3.2.1 The school provides access to the internet and associated technologies because it believes that it contributes positively to the teaching and learning process. It is expected that it will be used to benefit staff and students, but it is also understood that it may be used to engage in personal activities. All activity however should be appropriate to the school environment. This applies to school owned ICT devices used inside or outside of school, and personally owned ICT devices used inside school and during school activities.

3.2.2 The policy guidelines for teachers are provided for teachers to monitor their use of ICT. Teachers are responsible for all activity that is associated with their ICT account. They may not share their account details with anyone. To help maintain the security of their account, they must use a strong password, if they suspect that their account details are known by someone else, than they must let the ICT convener know.

3.2.3 In all use of ICT devices it is important that teachers relate to others positively, to avoid engaging in harassing harmful communications, to respect other people’s freedom and uphold their right to privacy.

3.2.4 The principles of confidentiality and privacy extend to accessing, inadvertently viewing or disclosing information about staff, or students and their families, stored on the school network.

3.2.5 Teachers should bear in mind that professional and ethical obligations are as applicable to activity online as they are to their daily interactions with students and the community in and out of school.

3.2.6 It is every individual's responsibility to ensure that when using ICT, their actions are within the law. This includes research, communications, use of social media, file sharing and any other activity carried out in the context of teaching and learning.

3.2.7 All ICT equipment should be used with care. If a staff member needs to install hardware or software and are unsure of how to do so, or are concerned about the effects that this may have, they must check with the school ICT convenor before they do so. If they know that equipment has been damaged, lost or stolen, they must report it as soon as they can.

3.2.8 ESI believes in the importance of developing confident and capable users of ICT. If staff members are unsure of anything regarding the use of ICT in teaching and learning, they should discuss this with the principal or head of department or ICT representative.

3.2.9 Should a situation arise that a staff member does something that constitutes a breach of this policy either accidental or deliberate, they must notify a head of department or principal as quickly as possible, they must make detailed note of the incident including time, date, names of those involved, any devices and their summary of the implications of the situation.

3.3 Responsibilities of the School

3.3.1 In the interest of maintaining a safe environment, the school reserves the right to conduct an audit of its computer network, internet access facilities, computers and other school ICT equipment. This may include any stored content, and all aspects of its use, including emails. An audit may include any device provided by or subsidised by/through the school or using school provided software. For this purpose, any electronic data or files created or modified on behalf of the School on any ICT device, regardless of who owns it, is the property of the school.

3.3.2 The school may monitor traffic and material sent and received using the school's infrastructures or devices at the school.

3.3.3 ESI believes that ICT is an integral part of teaching and learning, but is aware that when using it, the school may experience challenges from time to time. The school has a right to deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data. Filtering should enhance the teaching and learning process rather than restrict it. In situations where this is not the case, the staff member should inform the school rather than attempting to circumvent filtering or monitoring systems.

3.4 Responsibilities of Staff members.

The guidance that young people receive in their development of cyber skills is of the utmost importance. The success of their learning is greatly enhanced by the increased capability of the staff members around them. As a critical component in this process for students, it is important that the staff member understands what makes a successful cyber safety use.

- Staff should be knowledgeable about the technology that young people are using to enable them to discuss the way in which it is used and the challenges experienced.
- Staff should be aware of opportunities presented by technology in terms of its use in education, but also its use in other aspects of society including its social application.
- Staff should be aware and understand the challenges that exist around technology and how it affects the youth.
- Staff should act as a consistent and a positive role model for responsible activity online.
- Staff should be confident in their ability to make valued judgements about challenges and opportunities for students.
- Staff should discuss their own experiences regarding technology and share their strategies for managing challenges with their students. However, it is vital that they recognise the importance of consistent, positive role modelling in all of their use of technology in a teaching and learning context.

3.5 Breaches of this Policy.

3.5.1 A breach of this Policy by a staff member may constitute a breach of discipline and may result in a finding of serious misconduct. A serious breach of discipline would include involvement with objectionable material, activities such as abuse or harassment, misuse of the school's ICT in a manner that could be harmful to the safety of staff and students. This could question the user's suitability to be in the school environment.

3.5.2 If there is a suspected breach of this Policy involving privately owned ICT on the school site or at a school related activity, the matter may be investigated by the school. The school may request permission to audit that equipment/device (s) as part of their investigation.

3.5.3 In addition to any inquiry undertaken by the school itself, it may be necessary to notify a further authority in these matters, during or after the school's investigation.

4. Information and Communications Technologies Policy for Students.

When using information and communication technologies (ICT) at ESI, students will always use good cyber practices. This applies for school equipment/technology or use of private equipment/technology for any school related issue or any person associated with the school.

4.1 **Students must thus implement the following:**

- Be a confident and capable user of ICT – they must know what they do and if they do not understand about technologies that they use, they must get help where needed.

- Use ICT for learning as well as other activities- they must understand that technology can help them learn. They must also know it can also be used to talk to people, to buy and sell things and to have their opinion heard.

- Think carefully about whether the information they see online is true- they know that it is easy to put information online, and this means that what they see is not always right. They will always check to make sure information is real before they use it or share it with others.

- Be able to speak the language of digital technologies – when people communicate online, the things they share can be quite different from the conversation they might have if they were sitting next to each other. They must know that they must try to understand what people are saying before they react to them. If they are not sure they must ask someone else to explain.

- Understand that they may experience problems when they use technology- but that they must learn to deal with them or get assistance if relevant.

- Understand that there will be times when technology may not work as they expected it to or that people may be mean or unkind to them online- and when these things happen, they must know that there are ways they can deal with it. They must also know there are people they can go to, to get help if they don't know what to do next. Students may not get into physical confrontations about online communications.

- Will always use ICT to communicate with others in a positive, meaningful way – they must always communicate politely and with respect online. They know that it is possible to bully or hurt people with what they say or do on the internet. They must think about the effect that their actions have on other people. The relevant ICT device can be confiscated and the School's Code of Conduct implemented for perpetrators.

- Will be honest and fair in all their actions using ICT- they will never do anything online that they know will hurt someone. They must make sure what they do is not against the law. They must make sure that their actions don't break the rules of the websites that they use. When they are not sure about what they are doing, they will ask for help.

- Will always respect people's privacy and freedom of speech online- they understand that some information is private. They will be careful when using full names, birthdays, addresses and photos of other people and their own

4.2 **Implications of Misuse of ICT.**

Students must realise and take note that there will be consequences of not following this policy. These include but are not limited to:

- Following the stipulations of disciplinary actions of the School’s Code of Conduct.
- Providing the parents of the offended student (victim) with the details of the offender/s.
- Reporting to the SAPS or other relevant authority.
- Having their ITC device removed from them for a period of time.

4.3 School’s right to Investigate ITC Contraventions.

4.3.1 The Principal has the right to take any ITC device that a student has with them at school, if it is suspected that the student is contravening this policy or the School’s Code of Conduct. The Principal has the right to view and use such material if it is considered necessary.

4.3.2 The Principal has the right to request a student or parent to make any ITC device available to the school for inspections if is suspected that there is material that contravened this Policy

--- **---**

Signature **Date**