ST STITHIANS COLLEGE
ACCEPTABLE TECHNOLOGY & DIGITAL RESOURCE USAGE PROCEDURE

Introduction

This procedure is designed to ensure that the College's technology and digital resources are used in a responsible, ethical, and legal manner. It applies to all staff, students and members of our broader community who use the College's ICT resources, including but not limited to computers, networks, email systems, digital platforms, and internet usage. Our goal is to foster an environment that encourages the use of technology to enhance learning, while also ensuring the safety and privacy of all users. We believe that understanding and adhering to these procedures is a shared responsibility, and we appreciate your cooperation in creating a respectful and secure digital environment.

Please read this procedure carefully, as it outlines both acceptable and unacceptable behaviour concerning the use of the College's technology and digital resources. Violations of this procedure may result in disciplinary actions, up to and including termination of employment (for staff) or expulsion (for students).

Access to the College's computer systems and networks, including email, imposes certain responsibilities and obligations and is granted to users subject to the College's policies, procedures, and applicable legislation.
Educational institutions are constantly being challenged about how computers and personal devices including but not limited to laptops, smart phones, smartwatches, gaming computers, Virtual Reality sets and tablets can be used in constructive and educative ways, especially in classrooms and as part of learning experiences. At the same time, the College must manage the use of these devices to avoid the possible risks that can be incurred from careless or malicious use.

Acceptable use is always ethical. It should reflect academic honesty and demonstrate restraint in the consumption of shared College resources. It should ensure respect for intellectual property, ownership of data, system security mechanisms that are in place at the College and maintain individuals' rights to privacy.

Definitions

The following definitions bear the meanings assigned to them in this procedure:

1. "**College**" means St Stithians College, consisting of schools for students, from Grade RRR to Grade 12; Thandulwazi Academy is also included in the definition of the College;
2. **"Staff"** means persons employed by the College;
3. "**Head**" means the person appointed as Head of any one of the St Stithians College Schools or Departments;
4. "**Parent**" shall include:
    a) the biological or adoptive parent/s or legal guardian/s of a student attending the College;
    b) the biological or adoptive parent/s or legal guardian/s of a student enrolled, but not yet attending the College;
    c) the person legally entitled to custody or guardianship of a student, to the exclusion of the parent, without any rights to legal custody or guardianship;

3. “**Procedures**" means the documents which determine the governance and operational features of the College as approved and adopted by St Stithians College Subcommittees and/or the College Executive;
4. "**Student**" means:
    a) the child whose name appears on the Student Enrolment Form and whose parent wishes them to be enrolled in and educated at the College, irrespective of whether they are minors or not; or
    b) the child who, pursuant to an enrolment process, has been enrolled in and is being educated at the College, irrespective of whether they are minors or not.

Scope

This Acceptable Use Procedure (AUP) applies to all staff and students at the College (noting that guest users accessing our network via the Guest Wi-Fi, do so with specified rules and policy). This procedure governs the access and use of the College’s ICT resources, which include, but are not limited to:

1. **Computers:** All digital devices provided by the College for staff and students, including but not limited to desktop computers, laptops, and tablets;
2. **Networks:** The College’s internal networks, including Wi-Fi and wired connections, as well as remote access to these networks;
3. **Email Systems:** The College’s email system used for communication among staff, students, parents, and external parties;
4. **Internet Usage:** Access to the internet provided by the College, including streaming, browsing, downloading, and uploading content;
5. **Social Media:** The use of social media platforms for educational purposes, communication, and representation of the College. This includes, but is not limited to, platforms such as Facebook, Twitter, Instagram, LinkedIn, TikTok and YouTube
6. **Company-Owned Software and Other Hardware Infrastructure:** The use of software programmes, apps, and hardware infrastructure owned and provided by the College for educational and administrative purposes.

Please note that this procedure also applies to any personally owned devices used to access these resources while on the College’s premises or networks. It is crucial that all users understand and adhere to this policy to ensure a safe, respectful, and productive digital environment.

Authorised Access

All staff and students who have been granted access to the College’s ICT resources are considered authorised users. As an authorised user, you have a responsibility to help maintain the security of these resources.

1. **Protection of Login Credentials**: You are responsible for the protection of your login credentials. This includes creating strong passwords, not sharing your passwords with others, and changing your passwords regularly or as required by the ICT department of the College.

2. **Reporting Security Incidents**: If you suspect a security incident, such as a data breach or unauthorised access, it is your responsibility to report it immediately to the IT department or your relevant line manager or Deputy/Head of School, for staff or students, respectively.

3. **Understanding Your Role**: Every user plays a crucial role in maintaining a secure environment. This includes following this AUP, participating in any security training provided by the College, and staying informed about best practices for online safety and ethical digital citizenship.

By adhering to these guidelines, we can all contribute to the security and integrity of the College's ICT resources.

Unacceptable Use

The College is committed to maintaining a safe and respectful digital environment. As such, certain activities are strictly prohibited for all staff and students. These include, but are not limited to:

1. **Unauthorised Access**: Unauthorised access refers to any attempt to gain access to a College computer system, network, or resource without permission. This could include using someone else's login credentials, inadvertently or advertently making your login credentials available to others, exploiting security vulnerabilities to bypass access controls, or accessing data that you are not authorised to view.
2. **Confidentiality of Information:** While fulfilling their duties, staff of the College frequently encounter sensitive or proprietary data, which may include personal details about specific individuals, student records, or commercial information pertaining to business entities. Staff are strictly prohibited from accessing confidential data unless it is necessary for their job functions. Similarly, staff are forbidden from sharing any confidential information they have legitimate access to, unless their job duties require such sharing. These limitations are supplementary to any existing restrictions or prohibitions on the disclosure of confidential information under South African legislation.
3. **Distribution of Malicious Software:** This refers to the creation, distribution, or use of software that is intended to harm computer systems or data. Malicious software, also known as malware, includes a variety of forms such as viruses, worms, ransomware, spyware, and trojans.
4. **Distribution of Pirated/Counterfeited software**: The access of and/or distribution of pirated software is strictly prohibited under this Acceptable Use Procedure. Unauthorised copying, sharing, or selling of software not only violates copyright laws but also exposes users to significant security risks, including malware and data breaches. Engaging in such activities undermines the integrity of our digital environment and deprives software developers of their rightful earnings, which can hinder innovation and the development of high-quality software. Users are expected to respect intellectual property rights and support legitimate software distribution channels. Any violation of this procedure will result in disciplinary action, including potential legal consequences.
5. **Inappropriate Content and Conduct:** In accordance with the Film and Publications Act and the Sexual Offences Act, it is illegal for individuals under the age of 18 to engage in activities related to pornography. This includes viewing, possessing, downloading from the internet, trading, entering licensed premises where it is legally sold, or exposing another person under the age of 18 to such content. Child pornography, as defined by South African law, includes any explicit image displaying the genitalia of a person under the age of 18. Within our educational institution, the possession or distribution of pornography is viewed as serious misconduct. Any activities that involve viewing or circulating material considered pornographic, including but not limited to sexting, distributing explicit 'selfies', sharing explicit photographs/videos/voice notes of friends, or distributing photos/videos/voice notes of anyone involved in sexual activities, are strictly prohibited.
6. **Bullying and Harassment**

   The College maintains a zero-tolerance policy towards bullying and harassment. Unacceptable behaviours include, but are not limited to, the virtual attacking of members of the College or others on

any digital communication platform, cyber-bullying, insulting others, using racist or sexist language, or making derogatory or offensive comments.

Cyber-bullying encompasses behaviours that involve systematic, uninvited, repeated, and intentional abuse of another person over a period of time, causing harm to another person, inciting them to attempt to harm themselves, repeated threatening behaviour intended to frighten, hurt and or publicly shame or embarrass another person, or using digital technologies to spread rumours, share embarrassing pictures, videos, voice notes, websites, or create fake profiles. We are committed to fostering a safe, respectful, and inclusive environment for all members of our community.

7. **Academic Integrity**

   Plagiarism, or the presentation of someone else's work or ideas as one's own, is a serious violation of our institution's academic standards. This includes, but is not limited to:

   1. Representing information downloaded from the internet as your own work.
   2. Copying the work of another student.
   3. Presenting another person's ideas and/or AI-generated content as your own original thoughts.

   To maintain academic integrity, all information sourced from the internet must be properly cited. This includes providing the name of the website, the title and author of the article (if provided), and the date the information was accessed. Links to sources should also be provided. If AI is used, it needs to be explicitly acknowledged, and any requirements for its use mandated in teaching and learning adhered to. By adhering to these guidelines, we uphold the values of honesty, trust, fairness, respect, and responsibility in our academic community. Your cooperation in maintaining these standards is greatly appreciated.

Consequences

Violations of this Acceptable Use Procedure (AUP) are taken very seriously and may result in disciplinary actions, depending on the severity of the breach. These actions can range from a formal warning to more severe penalties such as:

1. **Disciplinary Actions**: For minor infractions, a formal warning may be issued. Repeated or more serious violations may result in further disciplinary actions, up to and including expulsion (for students) or termination (for staff);
2. **Account Suspension**: Depending on the nature of the violation, temporary or permanent suspension of access to some or all of the College's ICT resources may be imposed;
3. **Legal Measures**: In cases where laws have been broken, the institution may report the violation to law enforcement authorities, which could result in legal proceedings.

Please note that the institution reserves the right to determine the severity of AUP violations on a case-by-case basis. All users are expected to adhere to this procedure to maintain a safe, respectful, and productive digital environment.

Monitoring

The College reserves the right to monitor activities on all company resources. This includes, but is not limited to, computers and tablets, networks, email systems, and internet usage. The purpose of this monitoring is to ensure compliance with this procedure, protect our ICT resources, and maintain a safe and respectful digital environment.

Users should be aware that their actions on these resources may be subject to scrutiny. This includes, but is not limited to, websites visited, files downloaded, emails sent and received, and social media posts. Any activity that is found to be in violation of this procedure may result in disciplinary actions.

Please note that this monitoring will be conducted in accordance with all applicable laws and regulations to respect the privacy rights of all users.

Reporting Violations

The College encourages all users to report any violations of this Acceptable Use Procedure (AUP). If you witness or suspect a violation, you are urged to report it promptly to your relevant line manager or the ICT department or make use of the independent Whistleblower tip-off service. This includes any activities that you believe may compromise the security of our ICT resources, or any behaviour that is in violation of this procedure.

By reporting violations, you are playing a crucial role in maintaining a safe, respectful, and productive digital environment. Your vigilance helps us to address potential issues promptly and effectively, ensuring the integrity of our ICT resources and the well-being of all users.

Review, Governance and Updates

Ownership of this procedure and any subsequent policy is vested in the Head of ICT. This Acceptable Use Procedure (AUP) will be reviewed annually to ensure its relevance and effectiveness However, please note that it may be updated at any time to address emerging risks or changes in technology. The digital landscape is constantly evolving, and so are the challenges and risks associated with it. As such, the College is committed to staying ahead of these changes and ensuring the safety and security of our ICT infrastructure, resources and users. All updates will be communicated promptly to all users. We encourage you to review this procedure regularly and stay informed about any changes.

This Procedure is supported by or should be considered in conjunction with the following College policies/documents:

1. Whistle Blowing Policy
2. St Stithians Code of Good Practice (2007)
3. Employment Contract
4. Codes of Conduct
5. Learning and Teaching
6. Disciplinary Procedure Policy
7. AI Guideline (forthcoming)
8. Social Media Procedure
9. Social Media WhatsApp Guidelines

List of relevant legislation or policy applicable to this AUP:

1. The Protection of Personal Information Act 4 of 2013
2. Cybercrimes Act 2021

Original Version: Adopted & Approved by College Executive Committee: 09 MAY 2006

DECLARATION

PERTAINING TO THE ST STITHIANS COLLEGE ACCEPTABLE TECHNOLOGY & DIGITAL RESOURCE USE PROCEDURE (AUP)

I acknowledge and comprehend the terms and conditions of the Acceptable Use Procedure. I willingly grant permission to any authorised personnel employed by the College to oversee, intercept, and examine any communication or related information that may be present on the College's computer facilities. This includes, but is not limited to, e-mail and internet facilities, regardless of whether I am the originator of such communication or related information. This permission is provided as a broad consent and also as a specific consent under Section 5 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act No 70 of 2002.

_____

Name of Student

_____ _____

Signature of Staff Member/Student

Date