LEARNER ACCEPTABLE USE POLICY FOR THE INTERNET, SCHOOL NETWORK FACILITIES, SOCIAL MEDIA, INSTANT MESSAGING, ARTIFICIAL INTELLIGENCE AND PERSONAL DEVICES

Social media and general internet use is a valuable part of our society, and it is up to each individual in the school community to make best use of social media. The purpose of this policy is to ensure that Westerford High School's (the "School") internet, network facilities and all learner personal technological devices are to be used in a responsible and legal manner only. This *Acceptable Use Policy* provides a framework for the responsible and ethical use of technology, internet platforms and the school network in order to protect the privacy and ensure the safety of our staff and pupils.

For the purpose of this policy:

- "social media" refers to social networks (including, but not limited to, Twitter/X, Facebook and LinkedIn), media sharing platforms (including, but not limited to, Instagram, YouTube, Snapchat, TikTok and Pinterest), discussion forums (including, but not limited to, Reddit and Quora) and social blogging networks (including, but not limited to, Tumblr, Medium and WordPress)
- "instant messaging" refers to personal messaging applications including, but not limited to, WhatsApp, Facebook Messenger, Instagram and Telegram
- "network facilities" refers to information stored on the School servers and the school management software used by the School
- "device/s" refers to computers, mobile phones, smartphones, tablets, laptops or any other School or personal devices used by pupils for work or communication purposes
- "AI", or Artificial Intelligence, refers to computer systems that are designed to mimic human intelligence and perform tasks that typically require human intelligence, such as problem-solving, decision-making and content creation. It includes, but is not limited to, applications like Chat GPT that involves using a large language model, such as GPT-3, to generate human-like text responses to questions posed.

1. General Online Personal Safety

- Learners may not post personal contact information about themselves or other people on any social media or instant messaging platforms.
- Learners must not meet anyone they have met online without their parent's / guardian's approval.
- Learners must promptly disclose to a teacher any message they receive that is inappropriate or makes them feel uncomfortable. They should not show, send or forward the message to another learner.

2. Personal Device Safety while on the School Campus or on any school-affiliated tour or excursion

- The School will not be held liable for stolen, lost or damaged personal devices, including lost or corrupted data on those devices.

- The School is not responsible for maintaining or troubleshooting learner devices.
- Learners are responsible for the security and safety of their personal devices.
- Learners must ensure that their personal device is adequately protected from unauthorised use with, for example, a strong password, two step authentication or biometrics.
- Parents and pupils are responsible for adequately insuring any personal device brought onto the School property.
- Learners must limit the spread of electronic viruses and device exploits by ensuring that all personal devices have the appropriate, relevant and updated anti-virus software installed, where applicable.

3. Personal Device Usage while on the School Campus or on any school-affiliated tour or excursion

- Learners are responsible for their devices and anything that is done on, sent from or stored on that device.
- Learners should not share access to their device with anyone. Even a friend may do something on a device which is prohibited by this Acceptable Use Policy.
- Teachers have the discretion to allow and regulate the use of personal devices in the classroom and on specific projects. Learners will not use their devices in a classroom without permission from a teacher.
- Learner devices must be in silent mode while on the School campus, unless otherwise allowed by a teacher.
- Headphones or earphones may be used, only with teacher permission, while in the classroom.
- Headphones or earphones may not be worn in the school buildings. Learners may use your headphones or earphones before school, during breaks and after school when they are outside the school buildings.
- Learners may wear noise-canceling headphones in the classroom with the appropriate exemption obtained from the Wellness Department and supported by a recommendation from a Mental Health Professional.
- Learners must not use their device to cheat in exams or for the preparation and submission of any assignments.
- Learners must not use their device for non-instructional purposes during lesson time (such as making personal phone calls and text messaging).
- Learners must not use their device to record, transmit or post unauthorised photographic images or videos of a person or persons unless given express permission by the persons involved.
- Learners must not tamper with staff computers or staff devices.

4. System Security

4.1 Learners must not:

- attempt to gain unauthorised access to the Internet, the School computer network or the school management software used by the School.
- use another learner's account, log-in details, or password, or access another learner's files.
- give their log-in details and password to another person.

- print using another learner's account or Smart Card.
- make any deliberate attempt to disrupt the School's network or destroy data by spreading computer viruses or by any other means.
- eat or drink in the computer lab or near the printing facilities.
- change settings (such as screen savers or backgrounds on school computers or laptops) on any School devices.

4.2 Learners are responsible for their School network account and anything that is sent from or stored in that account.

4.3 Learners may only use the computer lab (and printing facilities) with written permission from a teacher and when it is not being used for teaching.

4.4 Learners should have no expectation of privacy in anything they create, store, send, receive or display on or over the school's various electronic systems, or the school's authorised third-party systems, including their personal files or any of the use of these systems.

4.5 Learners are expected to serve as positive ambassadors for the School and to be respectful in all communications (whether by word, image or other means).

5. The sending of emails to large groups

- Learners must not send emails to the global lists of learners or staff or groups. They should ask a teacher to do this for them.
- Cultural and Service Committees may not make use of the global lists to advertise events unless express permission is granted by the Senior Management Team of the School.

6. Plagiarism and Copyright Infringement

- Learners must not plagiarise third party works either in digital or printed form. Plagiarism is taking someone else's ideas and presenting them as your own.
- Learners must respect the rights of copyright owners. Copyright infringement occurs when you reproduce work without permission that is protected by a copyright.
- Learners must not download, copy or store any files obtained through illegal means (such as torrent sites or "free sharing" sites).

7. Fraud

- Learners must not tamper with, edit or change any documents sent out by the School, be these official documents like termly reports, or letters or any other form of communication or documentation.
- Be aware that tampering with, editing or changing official School documents or letters constitutes fraud- a criminal offence.

8. The use of AI

- Artificial Intelligence (AI) and AI-driven websites like Chat GPT have become increasingly popular within the educational context. AI should not be used as a substitute for a learner's own work but rather as a tool to enhance understanding of a subject.
- AI is acceptable to use in the classroom when the teacher explicitly approves its use.
- AI must only be used for homework and assignments if explicitly approved by the teacher.
- If AI is used, its use must be fully disclosed and referenced.
- Learners must not use AI to generate homework, or parts thereof, or assignments, tasks, projects or assessments, or parts thereof, without the teacher's approval and full disclosure. Doing so without approval will be considered cheating and will be subject to disciplinary action.
- Learners must not use AI for cheating, plagiarism, or any other unethical practices. It will be treated as a Serious Misconduct Offense under the School's Code of Conduct.

9. Inappropriate Access to Material

- Learners must not access material that is profane, obscene or sexually explicit (pornography), or that advocates violence or discrimination towards others.
- If a learner has mistakenly accessed inappropriate information, they must inform a staff member immediately.

10. Respectful Online Behaviour

- Whether sending public or private messages, posting on social media or participating in online discussion or debate, learners should take care with the language used and should share their views in a respectful, inoffensive and polite manner.
- **Everything posted and commented on social media, including instant messaging applications, is "published content" in the eyes of the law. The person who posted it, everyone who is a member of the group or followers of the poster, as well as everyone who read it, is part of the "chain of publication" and is collectively responsible for it.**
- **Should a learner object to a post or message, they must immediately register their objection and distance themselves from it by stating that they do not condone the content of the post or message. A person who fails to act, remains in the "chain of publication" and is as liable as the person who created or shared the post or message.**
- Be mindful that a statement made or image shared on social media or instant messaging applications may constitute the offence of defamation (damage to reputation or slander) or *Crimen Injuria* (infringement of dignity) and can be criminally prosecuted.
- Be aware that defamation or *Crimen Injuria* can be prosecuted even if the name of the person is not mentioned. If it is possible to correctly guess who is being referred to, the person who posted the message, as well as anyone in the chain of publication who did not object to it, is liable.
- Learners need to be cautious about what they post and share.

- Be cognisant of the fact that nothing on a Whatsapp group, even one between close friends, is private. Content shared out of a private Whatsapp conversation can still lead to disciplinary action.

Learners must not:

- post or share anything that could be received as offensive, defamatory, prejudiced, discriminatory or threatening by another person. They may have *meant* something innocently, but if it is received as offensive, defamatory, prejudiced, discriminatory or threatening, it will be treated as such.
- use any obscene, profane, lewd, vulgar, inflammatory, threatening, racist, sexist, or disrespectful language or images within any digital content.
- engage in personal attacks, including prejudicial or discriminatory attacks online.
- partake in improper communications, including, but not limited to, racism, hate speech, threats of violence or harm, incitement to any unlawful action or harm or violence, pornography, bullying or defamatory remarks.
- harass another person online. Harassment is acting in a manner that distresses or annoys another person. Stalking or trolling are examples of online harassment. If you are told by another person to stop sending messages to them, or about them, you must stop immediately.
- forward a message that was sent to you privately, without the consent of the person who sent you the message, unless it is to report the message as proof that an offence was committed.
- post personal information or pictures or videos of another person online or within the network for reasons other than direct educational purposes, and then only with their permission.
- alter or edit pictures or videos of another person for any intent other than direct educational purposes, and then only with their permission.
- post, forward, share, comment on, agree with or like a post or message that brings the name of the School in disrepute. A defamatory statement about the School, even if the name of the School is not mentioned but can still be correctly guessed, can be criminally prosecuted as defamation.
- The preferred method of communication between pupils and members of staff is email. Pupils should not contact their teachers privately on an instant message platform like Whatsapp.

11. Instant Messaging and Social Media Groups Related to the School

Learners shall:

- keep communication in groups for its intended purpose.
- not post personal information about yourself or others.
- not forward posts or messages from a group to anyone outside the group without the administrator's permission.
- exercise caution with forwarded items. Where possible, state the source.
- **not post improper communications, such as mentioned under clauses 9 and 10 of this policy.**

- distance themselves from improper communications as mentioned under clauses 9 and 10 of this policy and ask the administrator to remove it and address it with the poster.
- not use school-related groups for complaints against a parent, pupil or staff member (anyone contracted to or employed by the School). Use the official reporting channels of the School.
- leave a group at any time if posts are inappropriate or make a learner uncomfortable.
- not create groups or accounts on any social media or instant messaging platform that reflects the School's name or any affiliation with the School.
- not use social media platforms like Instagram for school-related communications and activities.

11. Disciplinary Consequences

- Violation of this *Acceptable Use Policy* is subject to the disciplinary process in the Code of Conduct and/or the Anti-Racism Policy, and may result in disciplinary sanctions or criminal prosecution.
- If a learner is found using their device during lesson time without the teacher's permission, the teacher may confiscate the device and only return it at a later stage. The length of confiscation will be determined by the number of similar prior offences.
- If a learner is suspected of transgressing this Acceptable Use Policy, the Principal (or their appointed delegate) has the right to confiscate the device and / or to investigate the account, email, documents, social media posts or instant messages related to the suspected transgression. A member of staff has the right to search the contents of a cell phone in terms of the searching procedures as described in the South African Schools Act.
- The School has a right, but not a duty, to inspect, review or retain any electronic communication created, sent, displayed, received or stored on or over the school's electronics systems; and to monitor, record, check, track, log, access or otherwise inspect the content of its systems.
- The School has the right, but not a duty, to inspect, review or retain any electronic communications created, sent, displayed, received or stored on users' personal computers, electronic devices, networks, internet or electronic communication systems; and also in data-bases, files, software, and media that contain school information and data.
- The School has the right, but not the duty, to inspect, review, or retain electronic communications created, sent, displayed, received or stored on another entity's computer or electronic device when users bring to and use such other entities' computers or electronic devices at a school location, function or event, or connect it to the school network and/or systems, or any system that contains school programs, or school data or information.
- Pupil Leaders, in whichever context within the School, are held to a higher standard. Any infringements of this policy, whether in a public or private capacity, may lead to the Pupil Leader losing their leadership position in addition to any other possible disciplinary sanctions.

Ratified by Westerford SGB: January 2024