ACCEPTABLE USE POLICY FOR THE INTERNET, SOCIAL MEDIA, INSTANT MESSAGING, NETWORK FACILITIES AND DEVICES

The Westerford High School internet, network facilities and all personal technological devices are to be used in a responsible and legal manner only. This *Acceptable Use Policy* serves to provide a framework for the responsible and ethical use of technology in order to protect the privacy and ensure the safety of our staff and pupils.

For the purpose of this policy:

- "the Internet" refers to the World Wide Web
- "social media" refers to social networks (including, but not limited to, Twitter, 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 and Telegram
- "network facilities" refers to information stored on the School servers and the school management software used by the School
- "devices" refers to computers, mobile phones, smartphones, tablets, laptops or any other School or personal devices used for work or communication purposes

1. General Online Personal Safety

- You may not post personal contact information about yourself or other people.
- You may not agree to meet anyone you have met online without your parent's / guardian's approval.
- You must promptly disclose to a teacher any message you have received that is inappropriate or makes you feel uncomfortable. You may not show, send or forward this message to another learner.

2. Personal Device Safety

- The School may not be held liable for stolen, lost or damaged devices, including lost or corrupted data on those devices.
- The School is not responsible for maintaining or troubleshooting pupil devices. Parents must pursue this with the place where the device was purchased or independent device specialists.
- You are responsible for the security and safety of your personal devices.
- You must ensure your device is adequately protected from unauthorised use with, for example, a strong password or biometrics.
- Parents are responsible for adequately insuring any device brought onto the School property.
- You 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

- You are fully responsible for your device and anything that is done on, sent from or stored on that device.
- Each teacher has the discretion to allow and regulate the use of personal devices in the classroom and on specific projects. You may not use your device in a classroom without permission from the teacher.
- Your device must be in silent mode while on the School campus, unless otherwise allowed by a teacher.
- Headphones may be used, only with teacher permission, while in the classroom.
- Headphones may not be worn in the corridors between lessons. You may use your headphones before school, during breaks and after school.
- You may not use your device to cheat.
- You may not use your device for non-instructional purposes during lesson time (such as making personal phone calls and text messaging).

- You may not use your device to record, transmit or post unauthorised photographic images or video of a person or persons on campus during school hours or during school activities, unless given express permission by the persons involved.
- You may not tamper with staff computers or staff devices.

4. System Security

- You may not attempt to gain unauthorised access to the Internet, the School computer network or the school management software used by the School.
- You are fully responsible for your account and anything that is sent from or stored in that account.
- You may not use another learner's account, log-in details, or password, or access another learner's files.
- You may not give your log-in details and password to another person.
- You may not print using another learner's account or Smart Card.
- You may not make any deliberate attempt to disrupt the computer system or destroy data by spreading computer viruses or by any other means.
- You may not eat or drink in the computer lab or near the printing facilities.
- During lesson time, you may only use the computer lab (and printing facilities) with written permission from a teacher and when it is not being used for teaching.
- You may not change settings (such as screen savers or backgrounds on school computers or laptops) on any School devices.

5. Bandwidth and Resource Violations

- You may not exceed your allocated weekly data.
- You may not send emails to the global list of learners or staff or groups without the express permission of a teacher.

6. Plagiarism and Copyright Infringement

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

7. Inappropriate Access to Material

- You may not access material that is profane, obscene or sexually explicit (pornography), or that advocates violence or discrimination towards others.
- If you have mistakenly accessed inappropriate information, you must inform a teacher immediately.

8. Respectful Online Behaviour

- Whether sending public or private messages, posting on social media or participating in online discussion or debate, you should take care with the language you use and share your views in a respectful, inoffensive and polite manner.
- Be cognisant of the fact that everything posted and commented on 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 responsible for it.
- Should you object to a post or message, you must immediately register your objection and distance yourself from it by stating that you 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 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.
- You may not use any obscene, profane, lewd, vulgar, inflammatory, threatening, racist, sexist, impolite or disrespectful language within any digital content.
- You may not engage in personal attacks, including prejudicial or discriminatory attacks.
- You may not partake in improper communications, including, but not limited to, hate speech, threats of violence or harm, incitement to any unlawful action or harm or violence, pornography, bullying or defamatory remarks.
- You may not harass another person. 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 him or her, or about him or her, you must stop immediately.
- You may not forward a message that was sent to you privately, without the consent of the person who sent you the message.
- You may not post personal information or pictures or video of another person online or within the network for reasons other than direct educational purposes.
- You may not alter or edit pictures or videos of another person for any intent other than direct educational purposes.
- You may not 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.

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

- Keep communication on groups for its intended purpose.
- Do not post personal information about yourself or others.
- Do 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.
- Do not post improper communications, such as mentioned under numbers 7 and 8 of this policy.
- Distance yourself from improper communications as mentioned under numbers 7 and 8 of this policy and ask the administrator to remove it and address it with the poster.
- Do 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.
- You may leave a group at any time if posts are inappropriate or make you uncomfortable.

10. Disciplinary Consequences

- Violation of this *Acceptable Use Policy* is subject to the disciplinary process and may result in disciplinary sanctions or criminal prosecution.
- If any pupil is suspected of transgressing the rules or the spirit of this Acceptable Use Policy, the Principal (or his 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.