Responsible Technology Use Policy - Students

There are six pillars to the **Responsible Technology Use Policy**:

RESPECT

Respect for self, for others, for property, and for rules and guidelines is a cornerstone of a strong, connected community.

REPUTATION

Anything posted online can go anywhere and find anyone. Content and context must be carefully considered every time technology is used to create, communicate, or publish anything. We should only post or share information that enhances the reputation of ourselves, members of our community, and the School. Our digital footprint matters.

RIGHTS

All members of our community have the right to learn and work in a safe, secure, and productive environment. Complying with copyright and licensing laws, and intellectual property laws, demonstrates respect for the rights of others.

RESPONSIBILITY

Every member of the School community is responsible for their use of technology and for the care and safekeeping of their phones, laptops and other devices. It is the responsibility of every user to ensure the protection of their identity and the security of their data.

GUIDANCE

The School supports the responsible and informed use of technology through ongoing dialogue, instruction, presentations, guidelines and essential agreements. All members of the School community are expected to model and support best practice in technology use at all times.

CONSEQUENCES

Technology use is a privilege. Misuse of technology may result in the suspension of privileges and/or disciplinary action by the School.

Responsible Technology Use Essential Agreement

As learners in the digital age, all students at Trafalgar Castle School are expected to demonstrate responsible technology use by:

- Respecting the rights of others;
- Adhering to copyright laws and other Canadian federal, provincial or local laws and statutes concerning the use of technology and intellectual property;
- Using technology only for appropriate purposes;
- Recognizing the need to protect online privacy and reputation;
- Monitoring and managing the amount of time spent online;
- Applying the School's Code of Conduct when using technology; and
- Accepting any consequences for the misuse of technology.

Students agree to:

- Refrain from the use of cell phones during the school day, except where permitted by School guidelines;
- Use private, strong and secure passwords, and not share passwords;
- Keep devices securely stored in a classroom or locker when not in use;
- Never hide, disguise or misrepresent their online identity;
- Pause and reflect before posting or sending any information online;
- Post only appropriate materials that will not cause harm to themselves, their family, others, or the School;
- Respect the confidentiality and privacy of others;
- Not represent the School or others in a negative light;
- Not access director or proxy sites that circumvent the security measures put in place by the School;
- Not download or install any unauthorized materials or software; not alter the configuration of School devices or remove pre-installed components without prior authorization of the IT Department; be responsible for all files, and maintain a backup of all work. Losing files is not an excuse for missing deadlines or not submitting work; and
- Understand and model all aspects of the **Responsible Technology Use Policy**.

Parents agree to:

- Monitor their daughter's online behaviours;
- Place age-appropriate restrictions and limits on their daughter's use of technology to support positive social relationships, sleep hygiene and mental wellness;
- Model and encourage responsible technology use and positive online behaviour;
- Support the School in its decision to limit cell phone use during the school day; and
- Support the School's **Responsible Technology Use Policy**.

Helpful tips for parents may be found here.

Faculty agree to:

- Model positive and professional technology use as outlined in the **Responsible Technology Use Policy**;
- Ensure that students have the requisite knowledge and understanding to use technology appropriately and effectively to enhance learning; and
- Support and monitor students' use of technology in the classroom.

Boarding Students

- Boarding students are authorized to utilize the School's Internet connection for recreational, entertainment, and personal use outside of their regular class hours, as long as all other policies are adhered to.

TECHNOLOGY USE INFORMATION AND GUIDELINES

Confidentiality

- The IT Department, as a result of performing its regular duties, has occasion to view the contents of a user's directories and any file stored in public space;
- All users must respect each other's right to privacy, which includes refraining from browsing or tampering;
- No person, regardless of status may view, change, copy or remove another user's files without the user's permission, whether the material exists on a shared computer, network media or on a student's own media; and
- Exceptions to user privacy exist where there is a just and reasonable belief that this Responsible Technology Use Policy is being violated, or where there is a runaway program which could be either an accidental or intentional intervention, or a virus is in the process of causing damage or is inhibiting the work of others, or when a public access workstation is being re-imaged as part of regular maintenance by the IT Department.

Inappropriate and Offensive Material

- Computing resources are not to be used to create, transmit, store, copy or access information that is obscene, threatening or harassing, nor should anyone be involuntarily presented with information, which the person transmitting it should reasonably know would be viewed by the recipient as offensive or insulting.

Recording and Transmission of Images

- The recording and/or transmission of images, audio and/or video without the consent of all those who are being recorded is strictly prohibited; and
- The use of any camera or recording device is banned in all areas of the School where there is an expectation of privacy including, but not limited to boarding areas, washrooms, locker areas, and change rooms.

Online Communication

- Communication sent from a school email account must be respectful;
- Inappropriate communication by students on social media or by email, even when such communication occurs outside the regular school day or is sent while not on school property or from a private device, may nevertheless result in disciplinary action by the School if the communication results in harm to other students or members of the school community;
- School administration reserves the right to audit any user's school email account if they believe a violation has taken place;
- Trafalgar Castle School will not regulate the content of private, consensual electronic mail communication between users; and
- All incoming and outgoing email is logged.

Internet Use

- Students may not use technology during class time without teacher permission;
- The Internet is to be used only for educational, instructional, research, and administrative purposes during the school day;
- The Internet offers access to information that is inappropriate, and students should seek advice from an adult in the school community if they have any questions about the appropriateness of material found on the Internet;

- Internet content filters are used to prevent accidental and intentional exposure/access to inappropriate content;
- Students must immediately inform the IT Department if they come across inappropriate content that has not been caught by the School's content filter; and
- All Internet traffic to and from the School's Intranet is monitored and logged.

File Transfer Protocol, Downloads and Peer-to-Peer (P2P)

- Networking/File Sharing is restricted on the Trafalgar Castle School network. In addition, it is the user's responsibility when downloading any file to check for copyright or licensing agreements, and adhere to the conditions outlined within.

Telnet, Remote Computing and Virtual Private Networks (VPN)

- When accessing remote computers and/or networks, the policies contained within the **Responsible Technology Use Policy** will apply. Where there are further restrictive policies in place at the remote facility, they will also apply.

Data Security

- The IT Department reserves the right to view and/or delete user files without prior notice to the user when the stability, integrity and/or security of the system are being threatened by actions on the part of that user; and
- The IT Department has the right to terminate any process when deemed necessary, and to delete any instance of virus in any file if it cannot be repaired.

Firewall / Content Filtering / Viruses

- The IT Department has the right to monitor any and all network traffic travelling via our Internet connection for improvement purposes or to ensure system integrity;
- The IT Department has the right to block any and all network traffic in violation of the **Responsible Technology Use Policy** using any means necessary;
- Individuals are responsible, and will be held accountable for any damage to data and files due to viruses they have introduced, either intentionally or inadvertently;
- The School is not responsible for any work, files or data that are lost, damaged and/or destroyed due to viruses introduced onto the network;
- It is the responsibility of individual users to maintain up-to-date antivirus software on their own computers, whether owned by the individual or assigned to the individual by Trafalgar Castle School; and
- The IT Department shall maintain antivirus software on public access, departmental and administrative workstations and on the network servers.

Remote Access

- Once users access the Trafalgar Castle School network remotely, all policies and procedures contained in this document will apply to the remote session.

Physical Facilities Security

- Digital hardware owned and/or administered by Trafalgar Castle School is, by definition, property of the School;
- No person or persons will, by any wilful or deliberate act, jeopardize the integrity of the computing equipment, its systems programs, or other stored information;
- All computing equipment must have reasonable physical security in place (i.e., reasonable measures to prevent theft and/or damage);

- Any action or attempt by a user to subvert or disrupt the functioning of any computer equipment is prohibited;
- No computing equipment or peripheral may be relocated, removed or reconfigured in part or in whole without proper authorization;
- Users are required to report any damaged or malfunctioning computing/networking equipment to the Information Technology Department immediately upon discovery to ensure prompt repair or replacement; and
- Any person or persons found to have damaged or who do not return any hardware for which they are accountable will be held financially responsible for its repair and/or replacement.

Software / Hardware Acquisition

- All computer resources acquired by the School are the property of the School and will be operated, maintained and administered by the School to maximize its benefits.