TRINITY GRAMMAR SCHOOL, KEW

Technology Acceptable Use Agreement

Why this agreement?

Trinity Grammar School aims to provide high quality educational programs in a caring, inclusive, happy andsafe environment.

Our technology programs, particularly the use of computers and mobile/digital devices, provide students, staff, contractors and authorised guests with powerful tools that expand learning and growth opportunities.

Along with these opportunities comes responsibility for all members of our community to interact with technologies in a way that is consistent with Trinity's core values.

As part of the Trinity community, you are expected to exercise sound ethics, integrity, empathy and judgement whenever you interact with technologies. Any actions which conflict with our core values - particularly those which harass other people or demean their dignity - are a breach of this Acceptable Use Agreement.

To whom and what does this agreement apply?

In this agreement, the term "user" or "community member" refers to any person, including students, teachers and educational support staff who access the School's network or who uses technologies provided by the School.

Although the policy often refers particularly to laptop computers, the same guidelines apply to the use of any computer or device in connection with the School. The Agreement also applies to use of personal or public technology devices whilst an enrolled student. Personal communications that are found to conflict with the School's values and thus breach Policy and Codes of Conduct will result in disciplinary action. This involves offensive, racial, harassing or demeaning communications within the Trinity community or against members of the general public.

We ask parents/guardians and students to read this Agreement and the Guidelines for Ethical and Responsible Use of Technology which is incorporated within the document.

Parents/Guardians must sign the policy electronically through Trinity Connect. There is no need to send a signed hard copy to the school. Before signing, we ask parents/guardians to discuss it with their child. We ask parents/guardians to satisfy themselves that their child understands the intention, detail and implications of this agreement at a level appropriate to their age.

TRINITY GRAMMAR SCHOOL, KEW

Technology Acceptable Use Agreement

I agree that, whenever I use technologies whilst enrolled atTrinity Grammar School:

- I will abide by this Agreement and follow the published Trinity guidelines for the ethical and responsible use of technologies;
- I will give due consideration to the dignity, feelings and well-being of others in all my electronic communications;
- I understand that the transmission or possession of offensive, inappropriate or objectionable material, including material infringing racial, sexual discrimination and harassment policies is against the law and accordingly I will not transmit or possess such material;
- I will not use a modern communication device to create, share, send or post messages of a sexual/explicit nature. I understand that this behaviour could lead to my enrolment being cancelled and serious criminal charges;
- I understand that I am responsible for all actions taken using my user account on a school computer/device or any other device;
- I will only use official school channels to communicate with members of the Trinity community;
- I understand that my network account (username and password) identifies me and that all communications (both internal and external) may be monitored, including the recording of video calls;
- I will ensure my username and password are secure and I will change my password regularly;
- I will not fraudulently use another person's computer/device, account, username or identity;
- I will not attempt to access or monitor information on any of the School's servers or any other person's computer without express permission to do so;
- I will not attend any online meeting if I do not have permission to attend from the meeting host;
- I will abide by Trinity's Wellbeing Policies as it applies to technologies and I understand that all cyber-bullying and offensive online behaviour against any person (including but not limited to that involving mobile devices, email, online chat, social networks and blogs) constitutes a serious breach of this agreement;
- I will not film, photograph or otherwise record a member of the Trinity community, whether student, staff, parent, contractor or visitor, without first seeking permission unless I have been authorised to do so as part of a properly conducted Trinity program;
- I will not share, publish or post film, photographs or other recordings without first seeking permission from those depicted and/or their legal guardians;
- I will not create, copy or post a virus or malware/spyware, or attempt to damage the network in any way;
- I will not use the network for any kind of commercial purpose without express permission to do so;
- I will not violate copyright law;
- I will not use any device in school, whether on the school network or otherwise, or any other school resource for gambling nor for accessing any pornographic material, nor for engaging in any illegal activities;
- While at school, I will exclusively access the internet via the school network;
- I will not attempt to bypass the school's security, nor mask my internet traffic using a VPN;
- I acknowledge that available technologies may be used for appropriate personal use outside the classroom whilst always acknowledging that their primary purpose is to support learning.

TRINITY GRAMMAR SCHOOL, KEW

Technology Acceptable Use Agreement

Guidelines for Ethical and Responsible Use of Technology: Being a GoodDigital Citizen

The following guidelines have been prepared to help you develop as a good digital citizen and understand your responsibilities when using technologies whilst enrolled at Trinity Grammar School, Kew.

Online Behaviour

- Behave online the same way you would offline or in person: treat everyone fairly and with common courtesy.
- Beware of giving out too much information about yourself or others online. Never share your username and password and change your password regularly. You should also:
  - Avoid posting personal information such as home phone numbers, addresses, school year levels and other identifying information about yourself or other school community members;
  - When communicating with people you have not met in the physical world, use non-provocative, ambiguous pseudonyms like "Basketball King 3", or "Minecraft Man 222". Avoid names like "tgsboy" which indicate that you are likely to be young and may give away your school.
- Take care to never leave a computer unattended while you are logged in. Press the Windows key and L to "Lock" your computer. You should never touch another person's computer without their permission.
- Be vigilant for phishing scams and never enter your password on a webpage that you do not trust.
- Be cautious of any site or person asking you to sign up for commercial agreements or financial transactions. Always check with a responsible adult before agreeing to purchase things online.
- Take care with the language you use online so that any messages you send do not offend, hurt or mislead the recipient or anyone else who reads it. If in doubt, say nothing.
- Be aware of the Trinity Harassment Policy (see front of the school diary) which promotes everyone's right to a safe and caring environment. Understand that this policy also applies to the online world; cyber bullying is unacceptablein any form.
- Remember that laws exist to protect people from receiving material which may be objectionable. The law includes all forms of communication including email, messages, and social media sites.
- Remember that photos, videos, recordings and text that you put online in any way can remain online, possibly forever. You have only limited control over what happens to media once it is online.
- Take the following actions if you have been harassed or bullied online:
  - Do not respond or reply
  - Save a record of the communication as evidence.
  - Tell a trusted adult (parent, teacher, etc.) as soon as possible.
- Be careful of websites which require you to submit your email address. Providing your email address on a commercial site puts you at risk of receiving a large volume of unsolicited email (spam) which may be offensive. Spam can also render your email account inoperable.
- If you come across offensive material on a website, exit the site and inform your teacher or another adult.

- You should not attempt to bypass Trinity's network security to access sites which have been blocked. VPN's and personal hotspots are not allowed to be used in School.

Use of School Communication Channels

(including Email and Microsoft Teams)

Personal exchanges are best handled in person. Avoid saying anything in an electronic communication that you would not say in person.

- All electronic communication between staff and students should be via Trinity systems such as your school email account, Microsoft Teams or myTGS.
- When a user sends any electronic communication, they are acting as an ambassador of the School.
- Correspondence should always be courteous and appropriate.
- Correspondence via school communication channels is not private. All email and Microsoft Teams messages are available to the system administrators when the school deems it necessary to investigate inappropriate behaviour. All communications sent via your school accounts are the property of the School and cannot be regarded as the private property of the individual who created it.
- Video conferencing using Microsoft Teams should only be initiated by a teacher/staff member. Students should leave a video chat when asked to do so by their teacher.
- Video conferencing meetings may be recorded by the teacher/staff member. The recording will be available in Microsoft Stream only to the teacher/staff member and the students who attended the meeting. The recording will be kept in Microsoft's secure data centres and will not be transmitted to any third parties.
- Students should carry out video conferencing in front of an anonymous background or utilise the 'blur my background' facility in Microsoft Teams.
- Students are encouraged to have a parent or guardian present during video conferencing sessions wherever this is practicably possible.
- Anonymous communications are prohibited, as is communicating using someone else's name or account details.
- Users should not attempt to join an online meeting to which they have not been invited. If you believe you have received an invitation in error, you should alert the sender.
- Users must not use their computer to create, save or send messages that contain offensive language, graphics, pictures, or attached graphics files or messages that are sexist, racist, or otherwise prejudicial or inflammatory. Whenever a member of the School Community is involved in sending such an email or communicating such information using the Internet (whether from inside school or beyond), it is considered a breach of the School's Technology Acceptable Use Agreement.
- Check your school communication channels regularly. Delete unwanted messages from your email inbox. You should also regularly open your Sent Items and Deleted Items folders and delete all unwanted messages. Email accounts are limited in size – to transfer large files (greater than 5 Mb), use the online file sharing service OneDrive for Business, which the School provides. Alternatively, a USB drive can be used.
- All email should include an appropriate subject heading.

- Users must not spam others. This includes posting unnecessary messages or sending or forwarding bulk or global emails. This includes chain letters, advertisements, or any other message intended to reach many different recipients without their consent. Students needing to send a legitimate email to a large group as part of an educational activity should do so with the assistance of a Head of Year, Head of House or associated Faculty Head.

Social Networking Sites and Chat / Instant Messaging / SMS

- Follow the online behaviour guidelines if you come across offensive/explicit material or behaviour.
- Make sure you know how to block unwanted messages and users.
- Protect your privacy and that of your friends and family by not giving out personal information.
- Check the information in your profile carefully to make sure your personal details are not available to strangers.
- Be especially careful not to 'geotag' photographs or other posts, as this can potentially reveal your location to strangers.
- Remember that once material has been posted online or sent electronically you lose control of it, and it may be used by others without your permission or in ways you did not predict.
- Learn how to make access to online profiles restricted so that only your friends can see them. You should always check the privacy settings for social networking sites but be aware that it is still very easy to copy or distribute material online.
- Check the privacy settings on services you use on a regular basis as changes in their policies may leave your private information exposed.
- Be careful when exchanging or downloading files: they can sometimes have viruses.
- You should not add people to your 'friends' or 'contacts' or 'buddy' list who you don't really know. Check that people who request to be friends with you online are who they say they are, perhaps by talking to them in person.
- Remember that your social media profile is only as secure as the security of your least secure online friend/contact.

Meeting someone from online

You are strongly advised against meeting anyone with whom you have only had online contact. If, however, you do decide to set up a meeting with someone you met online:

- Tell a parent/guardian and/or friends where you're going and let the person you're meeting know you've done this – any reason they want to keep the meeting a secret would be a suspicious one.
- Meet at your house while a parent/another adult who knows about it is at home, or in a public place where there are lots of other people (such as a shopping centre or cafe) and take a parent, or adult friend with you.
- Never, ever, agree to go to another place with the person who meets you – they could be leading you somewhere dangerous. Never get into a car with them.

Microsoft Stream

- Microsoft Stream is a video sharing platform, which is part of Office 365. It allows students and staff to share videos with each other or a subset of users.
- Users may only upload videos to Microsoft Stream that are related to their schoolwork.
- Users must not upload any videos to Stream which may be considered offensive, sexist, racist, or otherwise prejudicial or inflammatory.
- Users must not breach any laws of copyright when uploading to Stream.
- Users must seek the permission of persons included in any video before uploading it to Stream.
- Students are advised to set the permissions to their video so that only their teacher and other classmates can view the video.
- Any user who breaks any of these guidelines may have their access to Stream removed temporarily or permanently.

Mobile Device Use at School (including phones and smart watches etc.)

A mobile device is considered to be any electronic device other than the school provided laptop. This includes (but is not limited to) mobile phones, smart watches, iPads and other tablet computers, dedicated games consoles and any other internet connected devices.

During the school day* (from 08:15 am to 3:15 pm):

- All mobile devices must be turned off or on silent and locked in your locker. They may not be accessed during the School day;
- You may not use Facebook, Messenger, Instagram, Skype or other social networking apps on your school laptops and notifications must be turned off;
- You may not play computer games on your school laptop or any other device, unless instructed to do so as part of a proper teacher directed learning activity;
- At times teachers may require you to bring your mobile device (e.g. a phone) to class for a specific learning activity. You must then return your phones to your locker at the next available opportunity;
- Personal mobile devices that are connected to your school email account, online storage (OneDrive for Business) or other systems in school must be secured with a passcode or biometric security (e.g. fingerprint). The passcode must be required immediately every time you unlock your device. Your device must be set to auto-lock if left unattended.

** This timeline also includes when students are participating in school approved out of hours events, camps, tours and when representing the school out of hours.*

During Out of School Hours

- Students are required to accord with school enrolment and policy obligations when using technologies and communicating with mobile devices and personal technology devices.
- Any transmission of communications or material that are offensive, racist or demeaning and beach policy or the law will result in the student being subject to disciplinary review.

Downloading data

- Be aware that downloading large files from the Internet, streaming large amounts of media or participating in other bandwidth intensive activities can significantly impact and affect other users. Please be considerate in your use of these resources.
- Under current Australian law and Digital Rights Management (DRM), it is illegal to download or share copyrighted music, video and software without permission or without paying for them. Anyone who downloads files illegally or shares illegal downloads may be prosecuted.

Computer Care

Software and Configuration

The software supplied by Trinity in the original load must be kept on each laptop computer. Additional software can be installed using "Software Centre". The configuration of the machine must be maintained so that the computer and standard software is always available for use in class, and to ensure the School's network resources remain accessible.

Files and Back-ups

- Name your files and folders clearly and consistently. Keep file names short and avoid using punctuation in any file/folder names.
- You should regularly back-up your work. We recommend you use your school-provided OneDrive for Business account to back-up your files. OneDrive for Business gives you 1Tb of online storage and will automatically back up any files on your computer.
- Users can also use external drives such as USB drives to back-up their files. You should always keep back-up media in a different location from your computer. Never leave them in your computer bag. (After backing up, open the file toensure the back-up was successful.)
- All computers taken to the Trinity Tech Centre for repairs are assumed to be backed-up.

Care of Hardware

- Users are expected to take good care of all devices they use, both their own and the School's. Any problem with software or hardware with your school-issued machine should be logged promptly with the Tech Centre for attention.

- Restart your computer at least once a day at school. (Press start > power > restart). This will ensure you have the latest security patches and anti-virus updates. Note that updates are not installed when your computer is 'shut down' or in 'sleep mode'. Shutting the lid of the laptop does not restart the computer.
- Using stand-by mode throughout the day reduces the time it takes for your computer to be ready for work.
- It is your responsibility to ensure that, if you add personal files or software to your computer, it is still able to be effectively utilised in the classroom (students) / for intended work practices (staff). Installing games, fonts, "theme- packs" and software obtained illegally or for free is potentially dangerous and is likely to result in software problems with your machine. If you are unsure about the origins of a file, then do not install/copy it to your computer.
- All personal mobile devices are to be managed and secured by the student. The School accepts no responsibility for security, loss or damage of these devices.

Virus Protection and Security

- The school uses a suite of next generation Antivirus and firewalling tools to protect your computer. These are designed to protect you, your computer and, importantly, the school network from a variety of threats. These include viruses, malware, software with serious security vulnerabilities and other attacks. It will block any software from running that it does not trust. It will also block access to websites that should not be accessed in accordance with this agreement.
- You should not attempt to subvert, exit or uninstall any security measures provided by the school. Updates are installed automatically; you should ensure your computer is kept up to date.
- You must not run another anti-virus program. There is no need to install any other anti-virus software.
- If you believe a Trinity security system has blocked a piece of software or website that is safe, then please report this to the Tech Centre in person. They will always add safe software to the whitelist.
- Always allow Windows Updates – these updates are also important in protecting your machine from viruses as anti-virus software.
- If you are unsure about an attached file in an email, do not open it, especially if it is an executable (.exe) file or a zipped file (e.g. .zip). Office documents can have viruses embedded in them as macros (e.g. Word files ending in.docm), so be aware and be careful; only open macro enabled files from sources which you trust.
- If an email comes from someone you do not know or trust, delete it to avoid potential infection. Never open attachments from potentially untrustworthy emails.
- Be vigilant for phishing scams and never enter your password on a webpage that you have followed by clicking a link in an email.
- If your school username and password have been compromised, our account may be temporarily suspended automatically. If this happens, please visit the Tech Centre for assistance.
- Restart your computer regularly to keep windows up to date.