TRINITY GRAMMAR SCHOOL, KEW

Technology Acceptable Use Agreement

Why this agreement?

The mission of Trinity Grammar School includes high quality educational programs in a caring, inclusive, happy and safe environment.

Our technology programs, particularly those involving computers and mobile devices, provide students, teachers and educational support staff with powerful tools that expand learning opportunities.

At Trinity, you may also apply the variety of available technologies for appropriate personal use outside the classroom whilst always acknowledging that their primary purpose is to support learning.

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.

Who and what does this agreement apply to?

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

Although the policy often refers particularly to tablet computers, the same guidelines apply to the use of any computer or device in connection with the School.

I agree that, whenever I use technologies as part of the Trinity community:

- I will follow 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 of 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 communications device to create, share, send or post messages of a sexual nature. I understand that this behaviour could lead to serious criminal charges.
- I am responsible for all actions taken using my user account;
- I understand that my network account (user name and password) identifies me and that all communications (both internal and external) may be monitored;

- I will ensure my username and password are secure and I will change my password regularly;
- I will not use another person's 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 abide by Trinity's Harassment Policy as it applies to technologies and I understand that all cyber-bullying (such as that involving mobile devices, email, online chat, social networks or 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 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 the my mobile device, school network or other school resources for gambling, accessing pornography, sex chat, or illegal activities;
- While at school, I will exclusively access the internet via the school network;
- 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

This agreement exists as a set of guidelines to assist Trinity Grammar School to provide a safe and useful working environment for all computer users and the return of this signed agreement is a condition of continued use of the School's network resources.

The School's network resources are only made available to Trinity students (from Years 3 to 12) and staff after they have signed and returned this agreement.

We ask parents to read this Agreement and the Guidelines for Ethical and Responsible Use of Technology which accompany it.

Before signing this agreement, we ask parents to discuss it with their son. We ask parents to satisfy themselves that their son understands the intention, detail and implications of this agreement at a level appropriate to his age.

Declaration

I have read the Trinity Grammar School, Kew Technology Acceptable Use Agreement, understand the meaning of all rules and conditions and agree to abide by them and by the spirit in which they were written.

TRINITY COMMUNITY MEMBER:

Name: ________________________________ Form/Class: ______________________

Signature: ______________________________ Date: ___________________________

PARENT or **GUARDIAN** (for students only):

I have read and understood the Network Acceptable Use Policy for Trinity Grammar School, Kew.

I have discussed this agreement with my son and have satisfied myself that he understands its intention, detail and implications.

Signature: ______________________________ Date: ______________________

RETURN THIS PAGE ONLY

Trinity Grammar School, Kew

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

The following guidelines have been prepared to help you develop as a good digital citizen and understand your responsibilities when using technologies 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. Don't give out your username and password to anyone else, and regularly change your password. 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 "CricketEnthusiast", or "HomerSimpson195". Avoid names like "tgsboy" which indicate that you are likely to be young and may give away your school.
- Take care never to leave a computer unattended while you are logged in.
- Be cautious with 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.
- Be aware of the Trinity Harassment Policy (front of the diary) which promotes everyone's right to a safe and caring environment. Understand that cyber bullying or bullying is unacceptable in any form.
- Remember that laws exist to protect people from receiving material which may be objectionable. This includes emails, chat, social sites and mobile devices.
- Remember, photos, videos, recordings and text that you put online in any way 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 bypass Trinity's network security to access sites which have been blocked.

Use of Email

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

- All electronic communication between staff and students should be via your Trinity email account.
- When a user sends an email, he/she is acting as an ambassador of the school. Correspondence should always be courteous and appropriate.
- Correspondence via email is not private. All email is available to the system administrators when the school deems it necessary to investigate inappropriate behaviour. All email sent via your school email account is the property of the School, and cannot be regarded as the private property of the individual who created it.
- Anonymous email is prohibited, as is sending or receiving email using someone else's name/email account.
- 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, 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 email regularly and delete unwanted messages from your Inbox. You also need to 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 1mb), use a USB drive, SD card, or online file sharing service such as Dropbox or SkyDrive.
- Always include a subject heading and use appropriate language.
- Users must not send or forward bulk or global email. This includes chain letters, advertisements, or any other message that includes many different recipients without their consent. Students needing to send an email to a large group as part of an educational activity can do so with the assistance of a Head of Year, Head of House or associated Faculty Head.
- You should be aware that sending an email automatically transmits your email address to the recipient.

Social Networking Sites and Chat/ Instant Messaging / SMS

- Follow the online behaviour guidelines if you come across offensive material or behaviour.
- Make sure you know how to block unwanted messages and chat users.
- Protect your privacy and that of your friends and family by not giving out personal information.
- Check the information in your profile to make sure your personal details are not available to strangers.
- Remember that material posted online or sent by SMS may have a life of its own, and be used by others in ways you did not predict or allow.
- Learn how to make blogs or profiles restricted in access to only your friends, and how to block messages or users. You should always set your social networking sites to private but be aware that it is very easy to copy or distribute any online material. Check 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 be careful about adding people to your ‘friends’ or ‘contacts’ or ‘buddy’ list who you don’t really know.

Meeting someone from online

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

- tell a parent 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, adult friend or more than one friend of your own age.
- 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.

Mobile Device Use at School (including smartphones, iPads, iPods, Android devices etc.)

- The use of mobile devices (Bring Your Own [Optional] Other Device: BYOOOD) is acceptable when used for enhancing learning objectives. Personal use during class time is not acceptable. Use of these devices for personal use during the rest of the School day is to be avoided.
- Mobile devices such as smartphones, iPads and Android devices are to be used to augment the existing 1:1 school computer program. The school tablet PC is the primary academic device and is required for all lessons unless otherwise directed.
- Academic staff may ask students to explain how their use of mobile devices is enhancing their learning experience.
- Only give out your mobile number to people you know and trust.
- Don’t reply to messages from people you don’t know, including companies, which sometimes send SMS SPAM.
- Follow the online behaviour guidelines for treating people with respect.

Downloading

- Be aware that downloading large files from the Internet, listening to online radio stations, or participating in other bandwidth intensive activities can significantly impact and affect other users. Please be considerate in your use of this resource.
- Under current Australian law and Digital Rights Management (DRM) it is illegal to download or share copyrighted music, video and games without permission or paying for them. Anyone who downloads these 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 tablet/notebook/desktop computer. The configuration of the machine must be maintained so that the computer and standard software is always available for use in class, and so that the school’s network resources remain accessible.

Files and Back-ups

- Name files and folders clearly and consistently. Keep file names short and avoid using punctuation in any file/folder names.

- Each user should regularly back-up work. The network “U” drive is a good place to do this or online services such as dropbox.com or skydrive.live.com are useful alternatives.
- Users can also use SD cards or USB drives (available from the book room) to back-up to. Always keep back-up media (SD cards, USB drives, etc.) in a different location from your computer. Never leave them in your computer bag.
- After backing up, open the file to ensure the back-up was successful.
- All machines taken to the Trinity Tech Centre are assumed to be backed-up.

Care of Hardware

- Users are expected to take proper care of all devices at their disposal, 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 machine completely at least once a day at Trinity. This will ensure you have the latest patches and anti-virus updates. 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 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 (BYOOOD) devices are to be managed and secured by the student/staff member. The school accepts no responsibility for security, loss or damage of these devices.

Virus Protection

- All Trinity computers have the anti-virus software (Sophos) which operates whenever your computer is on.
- Sophos protects your machine from:
  - Network viruses
  - Email transmitted viruses
  - Virus transmitted via USB/CD/SD Card/other media
  - Spyware/malware
- Do not exit or uninstall the Sohpos anti-virus program. Updates are installed automatically.
- You are not able to run another anti-virus program concurrently with Sophos.
- Always allow Windows Updates – these updates are as 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. Word and PowerPoint documents can have viruses and spyware/malware embedded in them, so be aware and careful.
- If an email comes from someone you do not know, delete it to avoid potential infection.
- Using Sophos to scan your folders and files on a regular basis is recommended.

To scan your machine: right-click, open Sophos Anti-Virus. Follow on-screen instructions.