Acceptable IT Use Policy

The mission of Alphington Grammar School is to provide 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.
Along with these opportunities comes responsibility for all members of our community to interact with technologies in a way that is consistent with Alphington Grammar School's core values.
As part of the Alphington 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.

1. To Whom and what does this agreement apply?

1.1. In this agreement, the term "user" or "community member" refers to any person, including students, teachers, educational support staff and contractors who accesses the School's network or who uses technologies provided by the School.
1.2. 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.
1.3. We ask Parents/Parent Liaison to read this Agreement and the Guidelines for Ethical and Responsible Use of Technology which accompany it.
1.4. Parents/Parent Liaison sign the Policy electronically through EdSmart. Before signing, we ask Parents/Parent Liaison to discuss it with their child. We ask Parents/Parent Liaison to satisfy themselves that their child understands the intention, detail and implications of this agreement at a level appropriate to their age.

2. I agree that, whenever I use technologies as part of the Alphington Grammar community:

2.1. I will follow the published Alphington Grammar School's guidelines for the ethical and responsible use of technologies;
2.2. I will give due consideration to the dignity, feelings and well-being of others in all my electronic communications;
2.3. 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;
2.4. I will not use a modern communication device to create, share, send or post messages of a sexual nature. I understand that this behaviour could lead to serious criminal charges;
2.5. I understand that I am responsible for all actions taken using my user account;
2.6. I understand that my network account (user name and password) identifies me and that all communications (both internal and external) may be monitored;
2.7. I will ensure my username and password are secure and I will change my password regularly;
2.8. I will not fraudulently use another person's computer, account, username or identity;
2.9. 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;
2.10. I will abide by Alphington Grammar School's Bullying Policy as it applies to technologies and I understand that all cyber-bullying (including but not limited to that involving mobile devices, email, online chat, social networks and blogs) constitutes a serious breach of this agreement;

2.11. I will not film, photograph or otherwise record a member of the Alphington community, whether student, staff, parent/parent liaison or visitor, without first seeking permission unless I have been authorised to do so as part of a properly conducted Alphington program;
2.12. I will not share, publish or post film, photographs or other recordings without first seeking permission from those depicted and/or their legal guardians;
2.13. I will not create, copy or post a virus or malware/spyware, or attempt to damage the network in any way;
2.14. I will not use the network for any kind of commercial purpose without express permission to do so;
2.15. I will not violate copyright law;
2.16. 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;
2.17. While at School, I will exclusively access the internet via the school network; and
2.18. 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.

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

3.1. The following guidelines have been prepared to help you develop as a good digital citizen and understand your responsibilities when using technologies at Alphington Grammar School.

3.1.1. 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 “Cricket Enthusiast”, or “HomerSimpson195”. Avoid names like “agsboy” 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 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 Alphington Grammar School’s Bullying Policy which promotes everyone’s right to a safe and caring environment. Understand that this Policy also applies to the online world; cyber bullying is unacceptable in 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 Alphington Grammar School's network security (for example by using a VPN) to access sites which have been blocked.

3.1.2. 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 Alphington 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 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 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 5 Mb), use a USB drive, SD card, or online file sharing service such as OneDrive for Business, which the School provides.
- All email should include an appropriate subject heading.
- Users must not send or forward 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 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.

3.1.3. 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 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.
- 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/parent liaison 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.

3.1.4. Mobile Device Use at School during the school day (from 8:30am to 3:35pm):

- 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.
- 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, TikTok 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.

3.1.5. 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.

3.1.6. Software and Configuration:

- The software supplied by Alphington in the original load must be kept on each laptop computer. 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.

3.1.7. 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 to ensure the back-up was successful).
- All computers taken to the Helpdesk for repairs are assumed to be backed-up.

3.1.8. 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 Helpdesk 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 (BYOD) 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.

3.1.9. Virus Protection:

- All Alphington computers have anti-virus software Sophos which operates whenever your computer is on. Sophos is designed to protect you, 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.
- You will not be able to exit or uninstall Sophos. Updates are installed automatically.
- You must not run another anti-virus program concurrently with Sophos.
- If you believe that Sophos has blocked a piece of software that is safe, then please report this to the Helpdesk in person. They will always add safe software to the white-list.
- 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 careful, and 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.