ONETOWORLD Global Learning Access at Lilydale Heights

Terms and Conditions of the One-to-World Program

General

1. These conditions apply to information and communication technologies, devices, digital learning and social networking services provided by the College or used during school-related activities or accessed using the College networks or systems.
2. The College may provide updates to these Terms and Conditions as required. If so the school community will be notified through the school online systems. If you do not agree to, or cannot comply with the new conditions you must contact the College to discuss further actions. You will be deemed to have accepted the Terms and Conditions as amended if you continue to participate in the Program after any amendments are published online.

Bring Your Own Device (BYOD)

3. In accordance with the Education (General Provisions) Act 2006, the cost of providing instruction, administration and facilities for the education of students enrolled at State schools who are Australian citizens or permanent residents, or children of Australian citizens or permanent residents, is met by the State. However, parents/carers are directly responsible for providing personal resources for their children while attending school.
4. The College provides access to Internet, email, cloud storage, shared ICT networked devices and other school based specialist technologies, provided that they are used in a responsible manner for educational purposes only.
5. The use of e-books and other digital learning resources requires one-to-one access to a personal student computer device. This device must be fully functional and available to students at all times. We expect every student to have a Bring Your Own Device (BYOD) as per school requirements.
6. The College may allow students to bring and use their own portable computer device for general learning activities. Any such device is referred as **Bring Your Own Device** or **BYOD**. It must meet the College's administrative and technical requirements and be approved at the discretion of the College. Families must ensure that students have unrestricted access to their BYOD whenever it is required for learning purposes.
7. The College may allow BYOD Companion Devices to improve learning experience and enhance productivity and creativity. Companion Devices can be used in combination with student Primary Device or alone where appropriate for learning activities. Using BYOD as a Companion Device is subject to approval of the College and special administrative and technical requirements may apply.
8. The College may recommend to source a BYOD of a particular model(s) to ensure students have options which would best suit our curriculum and technical environment. If so the College provides reference to the online purchase system (LWT). Purchases made using this system are private financial transactions between you and the third party. Schools do not receive any commission or other benefit as a result of your purchases on this system. BYOD devices specified by school are subject to change based on availability.
9. Alternatively, you may source a BYOD of your choice as per minimal technical requirements provided in the BYOD Quick Specification Reference. These requirements are for reference and indication only. The College may not accept a BYOD if it does not meet the requirements. If a BYOD meets the requirements the College will apply reasonable efforts to configure and connect it to the College network but this may not be achievable and the BYOD may not be accepted.

School Loan Device

10. In some cases, the College may provide students with loan computer devices. These devices are referred to as **School Loan Devices**. The School Loan Device always remains the property of the College and it is subject to all conditions applicable to the use of the school property.
11. Provision of loan devices is at the discretion of the College and may necessitate additional conditions. The Security Bond may be required prior to access to a school loan device.
12. Students must return their loan computer devices and accessories at the end of loan period in the same condition or the Security Bond may not be refunded.

Ethical, Legal and Responsible Use of ICT Resources and Systems

13. Lilydale Heights College requires all students to use its ICT resources and systems in an ethical, legal, disciplined and responsible manner for purposes stated by the College staff.

14. Students and families must be aware that use of these resources is subject to the full range of laws and Lilydale Heights College policies that apply to the internet, communications and to the use of computers. Such law and principles include students' obligations in relation to copyright, plagiarism, intellectual property, breach of confidence, defamation, privacy, bullying/harassment, vilification and anti-discrimination legislation, the creation of contractual obligations, and other civil and criminal laws.

15. Lilydale Heights College's ICT resources and systems must not be used for unauthorised commercial activities and/or personal gain. Actions performed using Lilydale Heights College ICT resources must comply with the terms of any licence agreement for the use of software programs and other online resources.

Copyright and Intellectual Property Rights

16. Students must not, through the use of Lilydale Heights College ICT resources and systems, copy, download, store or transmit material which infringes copyright or the intellectual property rights of others without appropriate approval. Such material includes music files, movies, videos or any other form of media.

17. Students and families should be aware that actions performed using computer and network resources, regardless of any disclaimers that might be made, ultimately reflect on the College and community as a whole. This is particularly relevant where users post or submit material in a way that makes it publicly available over the internet.

IT Security and Privacy

18. Students have a role to play in ensuring the security and privacy of information generated, stored or transmitted by use of the ICT resources and systems. Students are issued with unique usernames and passwords, which must be kept strictly confidential at all times.

19. Students must protect ICT systems, digital information and account details/credentials as follows:

    - Choose a secure password which is changed regularly.
      A secure password is one that is difficult to guess, for example, containing a combination of letters and numbers and not simply a name or date of birth.
    - Respect the privacy and confidentiality of information that they may come across through access to the ICT resources and systems.
    - Download, install or use only authorised software.
      Students are not allowed to install software on school-owned computers if it is not licensed to the College.
      Students are not allowed to install software on shared computers unless it is required by the College staff.
    - Make sure that approved antivirus software is installed and up to date.
    - Report any breach or prospective breach of network security to the ICT Helpdesk, the appropriate technical personnel or the teachers.

20. Students must not act in a way which could result in a breach of security or privacy. In particular, the following conduct is considered unacceptable:

    - Disclosing your username and password details to another person.
    - Taking or distributing photos or video of others without their express permission.
    - Electronically publishing any material showing the College or its members without the permission of the Principal.
    - Disclosing other private or confidential information to unauthorised persons.
    - Utilising for any purpose private or confidential information accessed by accident.
    - Gaining unauthorised access to any ICT systems by any means.
    - Using Lilydale Heights College ICT resources to remotely attack or compromise other systems or networks.
    - Downloading, installing or using unauthorised software programs, including intended installation and propagation of computer viruses and other malicious programs.
    - Accessing or intercepting others' electronic communications and files without permission.

21. Students must not use Lilydale Heights College ICT resources and systems to make their personal information publicly available without prior approval. Where such disclosure is made in the authorised way (for example, by the use of email or an official website), students and families should be aware that invasions of privacy may sometimes occur and it is outside Lilydale Heights College's control to prevent such instances from occurring.

22. Students and families should be aware that some ICT resources and systems provided by the College utilise cloud technologies and storages such as Microsoft Office 365 including email and OneDrive. These storages may be located

overseas and be subject to foreign copyright and privacy legislation. The College does not store and does not require students to store private and confidential material on cloud storages. Students are reminded that email should not be used to send sensitive and confidential information. At the same time the College may have to use student names and dates of birth to create user accounts for approved cloud services. If so the College will make reasonable efforts to keep private information provided to a minimal level.

ICT System Administration and Privacy

23. Students and families must be aware that the operation and maintenance of ICT systems often requires the backup and caching of data, the logging of activity and the monitoring of general usage patterns and as such, complete confidentiality and privacy cannot be guaranteed. Lilydale Heights College may also be required to inspect or provide copies of electronic communications where required to by law, or where the auditing of use and investigation of possible misuses of ICT resources is required.

24. Students and families must be aware that a range of system administration tools and services may be used to access or collect data for use by the College to manage the One-to-World Program.
The College may access or collect such data as:

    - Computer device hardware and configuration details including serial number, MAC address, Operating System, installed applications, installed security certificates;
    - Internet, application and storage usage statistics for any student;
    - Any files on the shared storages controlled by the College and computer devices included into the One-to-World Program.

25. Students and families must be aware that a range of system administration tools and services may be used to perform remote configuration of and administrative access to student personal computer devices included into the One-to-World Program.
The College may apply system configurations and administrative actions as follows:

    - System re-imaging or re-installation.
      These operations will delete all files from a local computer storage. The College is not responsible for the backup of data on student personal computer device but will advise on how students can create backup copies of their files.
    - Deleting inappropriate content from shared or personal storages controlled by the College.
    - Creating local accounts with administrative permissions.
    - Including computers into computer management systems e.g. Microsoft Active Directory domain or System Centre Configuration Manager.
    - Remote installation and removal of the College configuration settings.
    - Remote installation and removal of applications that belong to the College.
    - Identifying the general location of the device.
    - Resetting password and limiting access to your account and the device.

26. Students are responsible for the backup of all data they have saved to their device. The backup of this data is the responsibility of the student and should be backed-up to an external storage device, such as external hard drive or USB flash drive.

27. The College takes its obligations under privacy law seriously and will never use or disclose any personal information inappropriately as per the privacy policies of the Department of Education and Training. These policies can be viewed online at http://www.education.vic.gov.au/pages/privacypolicy.aspx.

Care and Use of Computer Devices

28. Notebook/Tablet computer devices must be stored in a safe and secure place including being secured in lockers whenever they are not in the student's direct possession, such as at recess, lunchtimes and during PE and Sport classes. Portable computer devices should not be left unattended at any time.

29. A notebook/tablet computer device must be carried inside a suitable carry bag at all times, including travelling to and from school, preferably inside the school bag.

30. Students must not consume food or drink when using computers. Portable computer devices are to be kept away from the meals area, food, drink and hot/cold surfaces.

31. Students must not plug/unplug network and power cables, keyboards, mice and other peripheral devices, from desktop computers. Students should report damage or disorder to the teachers, the ICT Helpdesk or the appropriate technical personnel.

Power Management of Notebook and Tablet Computer Devices

32. Power setting and battery management is a student's responsibility. Students need to ensure that the notebook computer is charged overnight and brought to school each day with a fully charged battery.

33. No provision for charging will be available throughout the school day.

The Standard Operating Environment of the Student Device

34. A Standard Operating Environment (SOE) is a standard configuration of an operating system and its associated software. The College may apply SOE to BYOD limited to configuration of some OS settings and installation of some software to ensure appropriate level of security and functionality, including but not limited to:

    - Local accounts, groups and policies;
    - Wireless network configurations;
    - Antivirus and other security software;
    - Technical maintenance and management software;
    - Microsoft Office Suite.

35. Students should apply any configuration settings with caution. They must not change antivirus, security settings and modify local administrative account or security groups created by the College.

Technical Support Provided by the College

36. Students must report any connectivity problems with their BYOD to the College ICT Helpdesk. Staff at the ICT Helpdesk will attend to the reported problems and provide a temporary replacement unit if applicable.
    Students may only approach the ICT Helpdesk during the times and following procedures approved by the College.

37. The College is not responsible for program installation, system recovery, removal of viruses or other malicious software and other maintenance support of BYOD. However, the ICT Helpdesk may advise on possible solutions, assist with some technical issues and provide virus and malware removal tools as appropriate.
    The College develops and provides tools and facilities for self-servicing.

38. The Helpdesk may recall student personal device for some administrative and technical reasons such as

    - Enforcing these Terms and Conditions;
    - Changing wireless and printing settings;
    - Inspections when any security, copyright or privacy concerns arise.

    Notified students must bring their BYOD to the ICT Helpdesk the same day.

39. Devices that negativity impact the school ICT systems or other users will have their access to the network immediately removed until the cause is eliminated.

Breaches of these Conditions of Use

40. The breach of these Conditions of Use will be taken seriously and may result in disciplinary action.
    Consequences range from loss or restriction of access to the College core ICT resources and systems or One-to-World Program, to formal disciplinary action for breach of Student Code of Conduct. Cases of serious, deliberate, and/or criminal breach will be referred to external authorities and may result in civil or criminal proceedings.

Liability

41. The College and its staff will not accept any liability for the fault, damage, theft or loss of any student's BYOD. Students who bring their own devices onto the College site do so at their own risk.

42. By accepting these Terms and Conditions students and families agree that the College and its staff are not, and will not be liable or held responsible for any damages, loss, costs or expenses as a result of:

    - participation in the One-to-World Program,
    - use of the school ICT resources and services,
    - the College's decision to not accept a student device as a part of the BYOD Program.