

# ICT and eSafety Policy

current as of 15 October 2018

The overall aim of Victory Lutheran College is to provide a safe learning environment with an eSafe (electronically safe) culture which is in keeping with the values of the College. The objective of this Agreement is to ensure the safe and ethical use of ICT within the College community.

The College provides you with the opportunity to use ICT equipment/devices and gives you rights to use and access services on the College network. The College expects you to act responsibly as you would with all other College equipment and facilities. All students from Years 4 -12 have individual usernames on the College Network. Years 2 and 3 students are provided with unique email addresses but their use is strictly monitored by their teacher.

The conditions outlined in this document apply to the use of the electronic communication system at the College. Electronic communications include, but are not limited to, all internet, intranet and email activities and related applications. The authorised users of the College's electronic communication systems are required to comply with the Agreement.

Breaches of this Agreement can undermine the values of the College and the safety of the eLearning environment, especially when ICT is used to facilitate misconduct. Such a breach deemed by the College to be harmful to the safety of the College or its members, may result in disciplinary action.

Please note students are not able to commence using the College's computer network, internet access facilities, or other ICT equipment/devices as defined in this Agreement until the acknowledgement page of this Agreement has been signed and returned to the Administration Office.

## Definitions of terms used in this Agreement.

- **'eSafety'** refers to the safe use of the internet and electronic communication systems.
- **'Electronic communication'** includes, but is not limited to communication made by using ICT equipment/devices such as Internet, Intranet, email and mobile phone activities and related applications.
- **'ICT'** the term 'Information and Communication Technologies'
- **'ICT equipment/devices'** include, but is not limited to, computers (such as desktops, laptops/notebooks, ipads, PDA's), storage devices (such as USB and flash memory devices, CDs, DVDs, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other similar technologies as they come into use.
- **'Agreement'** means this Agreement and any related eSafety Policy and Agreement which may be developed by the College from time to time.
- **'Prohibited use'** means use of College ICT or privately owned or leased ICT on the College site or at any College-related activity, in a manner which is contrary to the terms of this Agreement
- **'College'** means Victory Lutheran College
- **'College related activity'** includes, but is not limited to, an excursion, camp, sporting or cultural event, wherever its location.
- **'Unacceptable use'** includes, but is not limited to, acts of a malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, deliberate defacement or damage to any ICT device or equipment, plagiarism, gaming, impersonation/identity theft, inappropriate use of email.

Your username gives you special privileges and responsibilities. Each user is responsible for how this is used. Before you are given access rights, you will need to agree to a number of conditions, which are outlined below.

## 1. Security

- 1.1. For security reasons we expect you to keep your passwords and network login details private. You need to keep all your drives and files secure, and prevent others from accessing your work without permission. You must respect the rights and privacy of others and under no condition access their network accounts though their password and login, or through unacceptable use or illegal means: eg Hacking.

## 2. Storage

- 2.1. Make sure to save all documents on your VLC One Drive. All documents will be continuously synced keeping you protected at all times where you have an Internet connection.
- 2.2. Shared documents will be stored using one of Microsoft Office's many platforms eg. OneNote, SharePoint, Teams etc. All Microsoft products are now cloud based constantly syncing to back up your data.
- 2.3. **USB** devices are accepted for school related resources/ documents to be stored on. These are not to be used to transfer games or music to and from the College network.

## 3. Internet

- 3.1. Internet access is provided to students for educational purposes. The College provides access to quality online information sources via the Intranet and Student Café for curriculum material etc. The allowance made to students for Internet use is generous, and appropriate for such educational usage. While the College has a large capacity connection to the Internet, downloading large files such as graphics, sounds and software will quickly use the data allocation provided to each student. **Downloading or streaming music and/or videos is forbidden.** Accessing online sites purely for personal use or entertainment (such as games) is also a breach of this agreement, unless approved by a teacher. Please speak with your Teacher or the ICT Support Officer about this if you are in doubt.
- 3.2. Use of file-sharing, torrents, VPN's, proxies are specifically banned and blocked by our system. BYOD students are not to use such services at school and should ensure they are disabled.
- 3.3. Access to the Internet via the College's facilities may not be used to browse, download or distribute material which is of an anti-social nature, pornographic, violent, illegal, racist, destructive, demeaning or denigrating of others or which encourages this. You must respect laws and other people's rights, including copyright laws and antidiscrimination laws. Use of social networks (such as Facebook), public chat sites and programs are not permitted. **All use of the Internet is recorded and the Information Technology Department can monitor all Internet sites visited by students should there be cause for concern. Random monitoring also takes place throughout the year. This also applies to BYOD students.**

## 4. Mobile Phones, iPods and other Personal Electronic Devices (PED's) and BYOD

- 4.1. The Administration Office is the appropriate means for contact between parents/guardians and children while the child is at school. Mobile phones are not to be used for this purpose. Permission to have mobile phones and PED's at

school or while under the College's supervision is dependent on the parent/guardian giving permission each year in the form of a signed copy of this policy for each child permitted to have these. Parents/Guardians may withdraw their permission at any time by notifying the College. All mobile phones must be switched off when the student arrives at the College, and must not be switched on again until leaving the College's supervision.

## 4.2 Mobile phones must not be connected to the College network and are not acceptable for our BYOD program.

- 4.3. **All students in Foundation to Year 6** must hand their PEDs in at Administration. **Secondary School students** may leave theirs in their lockers during the day. In cases where security is considered an issue, Secondary School students should hand PEDs into the Administration Office.
- 4.4. **Years 5-12 students** are required to participate in our **BYOD** program (optional for Year 4 students) and should familiarise themselves with the conditions and expectations outlined in our BYOD Handbook. These devices may be used by students throughout the day.
- 4.5. Staff are entitled to confiscate mobile phones or PED's from students who carry/use them during the school day. Students can collect these from Administration after school. Subsequent infringements will result in a parent/guardian being required to collect the device from the Administration Office.
- 4.6. **BYOD student devices can be confiscated** by staff if they're suspected of breaking this agreement in any way. Parents/Guardians will be asked to collect the device and discuss the suspected breach with the Head of School or Principal.
- 4.7. Personal music must never be listened to during class. Earphones or headphones must be carried by students, but only used if explicitly instructed to by a teacher for class purposes (not personal music). Year 11 and 12 may listen to personal and appropriate music stored on their device during designated study periods in Argus, but must never stream music or video.
- 4.8. Mobile phones and PED's are each student's responsibility. The College can not be held liable for damage, loss or theft.

## 5. Copyright

- 5.1. Copyright laws and licensing agreements must be respected and sources appropriately acknowledged and referenced. You are expected to abide by the Copyright Laws and licensing agreements. The fair dealing legislation allows student use of copyrighted materials provided they abide by attribution and referencing of materials.

## 6. Network Printing & Internet Use

- 6.1. The College provides network printers and Internet for student use. A reasonable print allocation and download limit is provided to each student. If this allocation is exceeded, the ability to print at school and browse the Internet will be suspended until additional print capacity is purchased by the student at the Administration Office.

## 7. Email

- 7.1. Email is only used in class time at the request of the class teacher or as required for school communication at home.
- 7.2 Use of public chat sites and programs is not permitted, unless agreed to by the class teacher. It should be noted that your

email address carries the College name. Therefore, the email network must NEVER be used to make comments that:

- (a) are rude, obscene or offensive, including discrimination against any person or group;
- (b) are discourteous to an individual or organisation;
- (c) might injure the reputation of another person or offend that person;
- (d) are trivial or likely to annoy the receiver.

## 8. Laptops/Personal Computers/Tablets/iPads/BYOD

- 8.1. Only students in Years 4-12 may bring a BYOD for school use.
- 8.2. Students in other year levels may be granted special permission by the Head of School to BYOD for special learning needs or circumstances.
- 8.3. If permission is given to bring a device to the College, it is agreed to use it only during school periods, for schoolwork only. Students will be personally responsible for preventing loss or damage to the computer.
- 8.4. Because of the requirements of the Victorian Curriculum and Assessment Authority, there may be instances when class work and/or assessment can not be completed using the portable computer. This will be decided at the discretion of the classroom teacher.

## 9. Privacy

- 9.1. The Privacy Act requires the College to take reasonable steps to protect the personal information that is held by the College from misuse and unauthorised access.
- 9.2. Whilst access to the facilities is provided by way of a personal account, authorised members of the College ICT Department reserve the right to investigate the way you use the facilities including email, network storage space and internet browsing.
- 9.3. It is understood that BYOD students will have personal information on their device. They are expected to manage this entirely. The College bears no responsibility for the misuse or unauthorised access of these devices.
- 9.4. **Personal Hotspots and bypassing the Victory internet filters and firewalls are specifically banned** whilst at school.
- 9.5. While after school use of technology by students is the responsibility of parents/guardians, College policy requires that no student attending the College may identify, discuss, photograph or otherwise publish personal information or personal opinions about College staff, fellow students or the College. This also applies to College related activities. Any breach of this whilst at school will incur College Behaviour Management Policy consequences. Breaches of this outside of school may involve College consequences and/or police involvement.
- 9.6. The College takes a strong position to protect privacy and prevent personal information and opinions being published over technology networks including Facebook, Instagram, YouTube, Twitter (and any further new technology).

## 10. eSafety

- 10.1. It is the responsibility of all students to be proactive to ensure their safety in online environments. The College provides education for students about safety with ICT. The following Code of Conduct provides some guidelines for use of the internet and electronic communication systems.