



ICT and Acceptable Usage Policy

Prepared by



Compass Education
JDLF International Pty Ltd
Email: legal@jdlf.com.au
Phone: 03 9005 5217
Postal: PO BOX 366, Balwyn North, VIC 3104
Head office: Level 2, 74 Doncaster Road, Balwyn North, VIC 3104

- 1.1. The purpose of this Policy is to ensure that all users of the Viewbank College network, including staff, students and guests, use the online and electronic services in alignment with their legal obligations. Additionally use of our online and electronic services should be ethical and consistent with the aims, values and objectives of Viewbank College and DET (Department of Education and Training).
- 1.2. Viewbank College is an educational institution, under DET, charged with the safety and education of students. It holds occupational health and safety obligations to its students and employees and must comply with State and Commonwealth legislation.
- 1.3. ICT resources must be properly and efficiently used. Viewbank resources and systems must not be used for inappropriate activities for example, pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment, including sexual harassment, stalking, privacy violations and illegal activity, including illegal peer-to-peer file sharing.
- 1.4. Due to the sensitive nature of information on our network and online and electronic services, the school must ensure that our online and electronic services are protected and risks to data damage or unauthorised distribution are minimised. Strict guidelines have been developed to ensure our network remains functional and secure.
- 1.5. Students must use school hardware and devices and ensure these devices are looked after and in a 'ready to learn' state (ie. charged and in working order).
- 1.6. In interacting with the worldwide community through electronic media, students' behaviour is expected to be an extension of the College Code of Conduct. Failure to follow the guidelines set out in this document will result in the loss of access privileges and may result in disciplinary action being taken where appropriate

- 2.1 Viewbank College is a community committed to learning. Copies of this policy are available online through the school's community portal, Compass. Alternatively, a copy of the policy can be requested by contacting the General Office during school hours.

This policy applies to all members of the Viewbank College community, including staff, parents, students and sub-contractors. It is the responsibility of Viewbank College community members to ensure compliance.

Depending on the nature of any inappropriate use or violation of this policy, non-compliance may constitute:

- i) a breach of employment obligations;
 - ii) serious misconduct;
 - iii) sexual harassment;
 - iv) unlawful discrimination;
 - v) a criminal offence;
 - vi) a threat to the security of DET ICT resources;
 - vii) a threat to the security of Viewbank College's network or electronic services;
 - viii) an infringement of the privacy of staff and or other persons; or
 - ix) exposure to legal liability.
- 2.2 Non-compliance with this Policy will be regarded as a serious matter and appropriate action, including termination of employment, suspension, expulsion, detention and/or other disciplinary action may be taken.
- 2.3 Where there is a reasonable belief that illegal activity may have occurred Viewbank College will report the suspected illegal activity to the police.
- 2.4 When using online services community members are representing the school and must ensure they uphold the schools values and expectations.

3.0 Learning and Business Purposes

- 3.1 When using digital technologies and school devices, both at school and externally, users agree to be safe and act in a responsible and ethical manner at all times.
- 3.2 Students will ensure that they:
 - 3.2.1 Protect their privacy; not giving out personal details, including their address, phone number, passwords or photos.
 - 3.2.2 Protect the privacy of others; never posting or forwarding their personal details or images without consent.
 - 3.2.3 Talk to a teacher if they feel uncomfortable or unsafe online, or if they see others participating in unsafe, inappropriate or hurtful online behavior.
 - 3.2.4 Carefully consider the content that they upload or post.
 - 3.2.5 Ensure they meet the terms and conditions of use for online services (including age restricted services). In the event they are unsure, a teacher should be consulted.
 - 3.2.6 Treat all school technology with care and notify a teacher immediately of any damage they cause or notice.
 - 3.2.7 Only use school owned devices when connecting to the Viewbank network.
 - 3.2.8 Will not install, distribute or play computer games on any school owned device.
 - 3.2.9 Will not interfere with network systems and security, the data of another user or attempting to log into the network with a username or password of another student, teacher or parent.
 - 3.2.10 Not bring to school or download any unauthorised programs.
 - 3.2.11 Not tether or connect to any non-school wireless access points (or hotspots) while on school grounds.
 - 3.2.12 Will abide by all copyright and intellectual property regulations.
 - 3.2.13 Will not connect any non-school owned device to the school network, including mobile phones, personal iPads or personal notebooks/laptops.

4.0 School-owned devices

- 4.1 Viewbank College is committed to ensuring the functional and safe operations of our school eServices and network. Accordingly, only approved devices are permitted to connect to our school network and for use within school grounds.
- 4.2 The use of non-school owned devices is strictly prohibited within the school and cannot be connected to the school network. This restriction prohibiting the use of personally owned devices assists us to ensure that:
- all devices are managed by our ICT department;
 - all devices have appropriate levels of insurance or warranty
 - we can provide site-licenced material to the devices, in alignment with our volume licence agreements
 - teachers can be confident materials will function and be available on the device
 - inappropriate use of the device can be tracked and identified
 - we can maintain appropriate levels of stock (or temporary replacement units), in the event a part or unit fails
 - units are repaired in alignment with servicing timeframes by authorised manufacturer technicians
 - we can confiscate devices in the event of inappropriate use
 - the school can authorise relevant repairs and warranty claims directly
 - liability may be limited in the event of accidental damage to another student's device as all devices are covered by group insurance, without the need to claim on personal insurance policies
 - periodic device certification and testing and tagging may be performed
 - appropriate anti-virus or anti-malware tools are running (ongoing or periodically).
- 4.3 All devices are covered by warranty for manufacturer defects and normal use of the device. In the event of negligence, abuse or malicious damage repair, replacement or excess costs may be payable.
- 4.4 Any problems, vandalism, damage, loss or theft of a device must be reported to the school immediately.
- 4.5 In the case of loss or accidental damage, a statement should be signed by a parent/carer and provided to the school.
- 4.6 Students may be required to replace lost or damaged chargers.
- 4.7 Students are responsible for ensuring their data is backed up and stored securely.

5.0 Rules for the use of technology

5,1 General

- The College reserves the right to check all electronic devices for inappropriate material.
- All laptops remain the property of Viewbank College until the final payment is made.
- All computer hardware is to be used for approved College work only.
- NO food or drink is to be consumed or placed near any computer.
- Non-educational games or music are not to be used on any computer.
- Students, parents/guardians and staff should adhere to the College Acceptable Use Agreement & Cybersafety Policy on the College website.

5.1 Security

Theft, Loss or Damage

In the case of **theft, loss or damage** the following conditions apply:

- The College must be notified immediately if a College-owned computer or device is lost, stolen or missing.
- It is the user's responsibility to report any lost or stolen computers or devices to the nearest police station and provide the college with a Police Report etc.
- A statement should be signed by a parent/carer and provided to the College.
- If the student's own device is damaged and the damage is not covered by the manufacturer's warranty the College will not replace the device. It is the student's own responsibility for their device.
- All users must log in under their own name and password and correctly log out at the end of each session. Students are responsible for information sent or accessed through their login details.
- Students must not attempt to discover, disclose or use another person's password nor must they reveal their own password to others.
- Students are not to tamper with the systems set-up or to add or remove software.
- There must not be defacing or damage to computer or learning device hardware or associated furniture.
- Vandalism is defined as 'any malicious attempt to harm, modify and destroy'; therefore it is strictly prohibited to vandalise any other user's data, the College network or other networks that are connected to the internet. This includes the uploading of viruses and attempting to hack into the College system.
- Students must get the permission of a teacher before entering a computer room used by another class.
- Students must not use any means, including suites or tools, to bypass internet security to access blocked sites.
- Whilst on College grounds, students will only access the internet via the College network.
- Students are not to be unsupervised in a computer room.

5.2 Printing

- On completion of work on the computer and printer, all paper, including printouts, must be removed or placed in the bin.
- There is to be no multiple printing. Students may print only one copy and should then use the photocopier for multiple copies.
- Documents should only be printed after the print preview has been used to check the document, a spell check has been done and the document / draft is completed.

6.0 Rules for Internet use

6.0 General

- Students may not upload to a website, or distribute electronically, any material relating to Viewbank College without permission from the Principal.
- The internet is to be used for approved College work only. Students must be able to demonstrate that the use is a valid component of research or class work, etc.
- The work of other persons is theirs alone. When using the internet as a source of information, a complete citing of the reference, including the web address and date accessed should be given. Plagiarism is unacceptable. If another person's work is used it must be acknowledged in accordance with copyright regulations. Students must not download or post information and assume authorship of the material. Copyright laws apply to certain websites – students must abide by copyright rules.
- Students are not to deliberately access, display, download or send unacceptable or illegal material (racist, sexist, violent, anti-social, obscene).
- If a student chances upon unacceptable material, he/she must switch the screen off and inform the teacher or librarian.
- Passwords are to be strictly confidential.
- No direct printing from the internet is to occur. Data is to be saved to USB, if required, before printing.

6.1 Communication via the Internet

- All students are expected to abide by the generally accepted rules of network etiquette and College Values. They must be polite when communicating with other people. This will include; not swearing, using vulgarities and inappropriate language, etc.
- Students must respect the College's rights relating to privacy and confidentiality. They must not give other people any information about themselves other than their name, email address and their College. Similarly they should not provide any information about any other member of the College community.
- Students are to avoid libellous criticism of other people or organisations. While debate is encouraged, libellous criticism can result in legal penalties. Students who are both directly and indirectly involved (through encouragement) of defamatory, libellous criticism and harassment via an electronic medium may be subject to disciplinary and/or legal (both civil and criminal) action. This extends to all content posted/submitted on social media websites, blogs, wikis, chat and other publicly accessible and restricted access websites.
- Students are not to access social networking sites.
- Students must not use the internet for any commercial purpose such as buying/selling of goods.