Monivae College

Monivae College Digital Technology Acceptable Use and Cyber Safety Policy 2014

This document applies to all users of the Monivae computer network and technology devices used at, or in conjunction with, Monivae College. This includes students, staff members and visitors to the College.

Further information on setting up and using the device is available provided via the College's self-help service http://helpdesk.monivae.vic.edu.au/selfhelp

Publication produced by the Monivae ICT Committee 2014
ict@monivae.vic.edu.au

January 2014

Digital Technology Acceptable Use Policy

Rationale:
Monivae College offers ICT to students and staff as a digital resource to enhance learning and teaching outcomes.

Policy:
All employees and students of Monivae College are responsible for appropriate behaviour while using the school's digital resources. It is expected that users will comply with legal, ethical and moral standards and the specific guidelines outlined within this document and in related policy documents. The use of the network is a privilege, not a right, and may be revoked if abused. The user is personally responsible for his/her actions in accessing and utilising the school's computer resources.

Guidelines:
Users are advised that some material accessible via the Internet and email may contain items that are illegal, defamatory, or potentially offensive. Monivae College has filter mechanisms that attempt to prevent access to inappropriate material; however, the user must ultimately be responsible for the correct use of the material.

Users must not attempt to by-pass the “filter mechanisms” installed on Monivae IT equipment. Any such attempt is considered a serious breach of this policy.

Users of Information Technology resources will be monitored by Monivae Information Technology Services (MITS). This includes any email communications and any data stored on IT related devices. Monivae College reserves the right to view and monitor any information transmitted using College hardware or within College boundaries. This includes personal emails received and sent on the school’s computers and/or network facilities.

Network accounts are to be used only by the authoriSed user who is deemed and held responsible for the contents and use of that account. Users shall not make available their logon name and/or password to others. Users shall not intentionally seek information about, obtain copies of, or modify files, data or passwords belonging to other users. It is inappropriate for a user to log on using the password of another person.

The use of information technology resources shall not disrupt the use of these resources by others. Hardware and software should not be destroyed, modified or abused in any way. Persons responsible for such damage or destruction will be subject to disciplinary action and liable for any cost of repair. Any damage to information technology resources must be reported to the MITS via teaching staff.

The IT devices provided by Monivae College are intended principally for Monivae College related work. Specifically, the use of information technology resources for the following activities is prohibited:

- Commercial or profit making purposes.
- Product advertisement or political lobbying.
- Composing, copying or distributing hate mail, discriminatory remarks, and other anti-social communications.
- Accessing, copying or publishing pornographic or other inappropriate or offensive material.
- Malicious use of information technology resources to develop programs

to infiltrate the College's or other computer system. The act of hacking/cracking may result in reports being made to law enforcement authorities.

Software unrelated to the curriculum is not to be installed, used or copied from or to information technology resources unless authorisation has been received from MITS.

College email will only be used primarily for legitimate school purposes. Users should direct the bulk of personal email to an account other than their Monivae account.

MITS reserve the authority to prohibit other activities that would reasonably be deemed to be outside the spirit of this and related policies.

Cyber Safety Policy

Rationale:
The Monivae College code of conduct should be applied to all areas of the curriculum including the use of digital technology. Thus the items specifically listed below should be taken as an extension of the college code of conduct forbidding and working to prevent the practices of bullying and harassment.

Cyber Bullying involves the unwanted use of electronic equipment devices to harass and cause discomfort to other members of the school community. Cyber safety refers to safe and desirable practices in the use of electronic and ICT equipment devices including but not limited to computers (such as desktops, laptops), storage devices (such as USB and flash memory devices, CDs, DVDs. Floppy disks, 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 technologies as they come into use.

Policy:
The use of ICT and other equipment/devices within Monivae College should be limited to educational and creative purposes appropriate to the school environment.

Guidelines:
The use of privately owned ICT equipment/devices on the school site or at any school related activity must be appropriate to the school environment. They should not contain information that would be considered as inappropriate given the Monivae code of practice. If at any time a user is unclear about whether an IT related activity is permissible or not, they should seek clarification from the Director of Studies or an appropriate proxy.

The school will take all reasonable steps to:

- Filter screen content being accessed through information systems such as the internet.
- Ensure that all material being accessed on the internet is appropriate and does not breach the guidelines outlined in this policy.
- Seek clarification with regard to accessing websites or other sources of information where the content may breach the guidelines outlined in this policy. This clarification may come from the staff member who is supervising at that time.
- Ensure that communications between students and other students, staff members and members of the outside community do not have the effect of harassing, vilifying or attacking personally other individuals.

This includes but is not limited to written words and the posting of images.
- Ensure there is appropriate follow up where instances of online harassment are found to have occurred.
- Implement the Monivae College approach to working through harassment or bullying issues.
- Work in a partnership with parents to investigate online harassment and to promote cyber safety in the school community.
- Utilize student support structures and counselling to provide all necessary support where instances of harassment or bullying have been found to occur.

College email should be used primarily for legitimate school purposes. Email facilities should not be used to:

- Bully, abuse, vilify, defame, harass or discriminate (by virtue of sex, race, religion, national origin or other).
- Send or receive obscene or pornographic material.
- Harm the reputation of the College.
- Spam or mass mail or to send or receive chain mail.
- Perform any other unlawful or inappropriate act.
- Transmit viruses, worms, trojans, bots or other malicious software.

Users must report any offensive or disturbing communications such as those mentioned above. This includes communications received out of school time.

Users should be aware that sending personal details across the network/Internet could lead to unwanted consequences. The College will not be responsible for the consequences of such activity.

Where the user is a student, parents are asked to:

- Monitor home use by students and report to the school any communications that may have breached this acceptable user policy.
- Ensure that ICT equipment/devices are placed in a position within the home where easy monitoring is possible.
- Support the college in encouraging responsible communication using ICT equipment/devices.

Cyber Safety Procedures

School based actions and consequences for breaching cyber-safety codes of conduct.

Monivae College will take the following steps where instances of harassment or bullying have been found to have taken place.

Step One: The students involved in the harassment are identified.

Step Two: The Student identified as the bully or the party responsible for harassment of another is interviewed. During this interview the impact of the bullying behaviour is made clear.

Step Three: Any further instances of bullying result in the perpetrator being subject to the formal code of conduct of the college. This involves a scaling up of consequences from “in school suspension” to an enrolment review meeting.

In general the school computer system shall not be used in any manner that will

harm other people or their property, interfere with the operation of the network or in any way violate any laws. All users will be held accountable for their actions and may incur a loss of privileges if the guidelines of appropriate use, outlined above, are violated.

Consequences for misuse of the system include:

- Exclusion from the Internet / email / entire network (either for a given time period or permanently)
- Financial responsibility to reimburse the school for equipment / time needed to rectify a problem caused by misuse.
- Expulsion / dismissal from Monivae College.
- Being placed in the hands of the police. (Attempting to “hack” a network system is a federal offence.)

Monivae College Digital Technology Acceptable Use and Cyber Safety Policy 2014

(To be completed by students and parent/guardians)
Agreement to abide by and support the Monivae College Digital Technology Acceptable Use and Cyber Safety Policy
We, the undersigned, accept and agree to abide by and support the procedures contained in the Monivae College Digital Technology Acceptable Use and Cyber Safety Policy, as well as any reasonable extension to this policy.
Name of Student:
Signature of Student
Name of Parent / Guardian:
Signature of Parent/Guardian
Date: