Guidelines for Ethical and Responsible use of Technology

Introduction

The following guidelines have been prepared to help members of the Koonung community understand and meet the expectations for responsible and ethical behaviour when using technologies associated with Koonung Secondary College. These guidelines sit within the parameters of the Student Engagement Policy and the Cyber Safety Policy. These policies are designed to enhance self-discipline and respect for the rights of others. It promotes an environment which maximises the opportunity for all student to achieve their potential.

Core expectation

Koonung Secondary College is committed to providing a computer network and digital resources which promote educational excellence and facilitate resource sharing, innovation and communication. The resources and our curriculum programs provide students, teachers and support staff with powerful digital tools that expand learning opportunities.

Associated with the opportunities that a digital teaching and learning program allows, is the responsibility for all members of our community to interact in a positive manner with the digital technologies provided. Sound ethics, integrity and good judgement are expected when interacting with all digital devices provided by Koonung Secondary College.

The College will be vigilant in managing student use of the digital resources to improve learning outcomes. Misuse of any digital resources provided by the College will be dealt with in an appropriate manner.

Policy Guidelines:

Before using the digital resources within Koonung Secondary College students must read the following guidelines and, together with their parent or guardian, sign the attached agreement.

General classroom etiquette and network security:

All members of the Koonung Community will:

1. Respect computer network security and the data of another user (including individuals, the school and the department) and only log in using their own login code and password
2. Download and run only authorised programs, learning games, and maintain settings for virus protection, spam and filtering which have been set by the school and/or department
3. Avoid all potentially offensive sites and refuse to be guided to these sites by others
4. Seek teacher or parent advice if unsure regarding about internet content or search methods, hostile or unpleasant emails, blogging or wiki content
5. Ensure that external data storage devices do not contain any programs or files which may cause harm or contain offensive material
6. Understand that their network account (username and password) identifies them and that all communications (both external and internal) may be monitored
7. Take care that their password is private and confidential and not shared with anyone, and adhere to the rules of changing their password regularly.

8. Not attempt to access or monitor information on any of the school's servers or any other person's digital device.

9. Protect personal privacy rights and those of other students or teachers by not giving out personal details such as: full names, telephone numbers, addresses and images (this includes school details).

10. Use the training/learning offered by the College to recognise other users' intellectual property and acknowledge these sources (in a bibliography including all text, images, and multimedia) where these sources have been used.

11. Not participate in cyber-bullying practices by reading or forwarding material that may be interpreted by others as bullying material and report this material to a teacher.

12. Students are expected to access and use digital devices under teacher supervision on the understanding that the primary purpose of the device is to support learning.

Online etiquette (manners) Social Networking sites and chat/instant messaging

13. Behave online in a polite and fair manner at all times, online manners are very important. Your words may be easily misunderstood or misinterpreted, so be considerate and tactful.

14. Check the information in your profile to make sure your personal details are not available to strangers. Blogs and profiles should be available to your friends only.

15. Respect the rights of others in all collaborative, online communication forums and email by using language which is polite and professional.

Downloading and Uploading:

16. If material you download offends anybody else – it is your responsibility and you may have to face consequences. Laws exist to protect people from receiving material that may be rude and offensive. You may not think it is offensive, but someone else might be offended by it.

17. Remember, photos, videos, recordings and text that you upload to sites in any way (even on secure sites) can remain online forever. Once you upload content you lose control of it. It can be accessed for personal or commercial (advertising, marketing) purposes by anyone.

18. If a site has been blocked and you consider this site to be of educational benefit – inform your teacher. Do not bypass Department / school network security to access games, music or social networking sites whilst at school.

19. Do not download blocked content at home and access them from your hard-drive whilst at school.

20. The Australian law and Digital Rights Management (DRM) states that it is illegal to download or share copyrighted music, video and games without paying for them. Downloading these files illegally or sharing illegal downloads is breaking the law and may be prosecuted.

Use of Email and security:

21. When emailing: Imagine that you are speaking to the person and type a polite version of what you would say. Capitals are considered yelling.

22. Email is for communicating information and sending documents. Do not become involved in email arguments. If an email exchange is becoming less than friendly, then end it and speak to the person in person and or consult a parent or teacher.

23. Take care with your email account. Don’t give out your email address to unreliable sites or your ‘in box’ may fill with SPAM (junk email – advertising).

24. Users must only send emails from their own named accounts. If you create an anonymous email account (ie: likered@gmail.com) account and send inappropriate emails from this account you can be tracked. Anonymous emailing such as this is prohibited.
25. Do not open emails which request that you update certain programs such as ‘flash’ and ‘iTunes’. Requests to update will generated from the programs themselves and will never be emailed. Do not open emails which promise gifts and opportunities. Simply opening these emails (not even the attachments) can release viruses/Trojan horses into your computer.

26. Users must not use their digital device to create, save or send messages that contain offensive language, graphics, images, or attached graphics files or messages that are sexist, racist or otherwise prejudicial or inflammatory (intended for impact and strong reaction). 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) it is considered a breach of the Acceptable Use Agreement.

27. Email accounts are not designed for storing information. You need to save important information as documents on your hard-drive. Your Koonung/Gmail account may delete emails automatically after 30 days. Clean out your deleted messages and sent mail boxes every fortnight.

**Procedures for breaches of the Policy Guidelines**

The College will be vigilant in managing student use of the resources to improve learning outcomes. Misuse of PC’s, laptops, Notebooks, MAC’s and other mobile ICT devices such as cameras will be dealt with according to the nature of the infringement.

Breaching the conditions stated in the *Guidelines for Ethical and Responsible Use of Digital Technologies*, the *Acceptable Use Agreement* and the *Cyber Safety Policy* may result in access restrictions and/or withdrawal of access to digital resources. The exact response or consequence to breaches will vary according to the nature of the infringement.

**The following are considered major breaches:**

1. Endangering the health and safety of others or the property of others
2. Vandalising the property of others
3. Harassing or bullying others
4. Downloading, displaying, saving, or transmitting any material that others may find offensive. This includes violent, racist, sexist material and pornography
5. Bypassing filters and network security with the intention of changing settings and or interfering with existing sites
6. Using someone else’s password to access email, intranet/Ultranet profiles or other online forums under their identity
7. Knowing about and failing to report or encouraging any of the above infringements to a teacher/co-ordinator or member of the Principal team.

**Procedures and consequences for breaches:**

In the event that a student is in breach of these guidelines the relevant Sub-school Managers should be informed. After consideration of the breach the person may have one or more of the following bans imposed:

- Temporary ban on using computers or mobile ICT devices
- Removal of email privileges and/or internet and network access
- If equipment and/or notebook is damaged the student will be asked to pay all associated costs in replacing or repairing the damaged equipment
• Removal from classes where computer use or mobile ICT device is involved
• Suspension or expulsion
• Authorities such as police may be contacted where the law has been breached

The following are considered minor breaches of the policy guidelines:

1. Playing games
2. Straying to sites irrelevant to the learning
3. Communicating digitally when not relevant to the requirements of the learning task
4. Disseminating irrelevant material
5. Failing to follow fair and reasonable instructions such as closing the netbook
6. Changing settings for virus protection, spam and filtering that have been set as a departmental or school standard

Minor breaches will be dealt with by the classroom teacher according to the established procedure which includes; a reminder of expected behaviour in the form of a warning, and the student temporarily logging off and completing the task without using digital technology.

Where a student repeatedly breaches, or commits multiple minor breaches, the student will be sent to the sub-school co-ordinator. An incident report will be completed by the student and teacher. Students will incur one or more of the above consequences at the discretion of the teacher and sub-school co-ordinators.

All technology (including Notebooks) remains the property of Koonung Secondary College. All accidental damages should be reported to the ICT Help Desk immediately or as soon as possible. Damages resulting from what is deemed ‘ongoing carelessness,’ will be dealt with on an individual basis.

Acknowledgements; Trinity GS, BoxHill SSC

Refer to following documents:
Cyber Culture Policy
KSC Style Manual
KSC KCreate or Senior_Shift Acceptable Use Agreement