ETHICAL and RESPONSIBLE USE of DIGITAL TECHNOLOGIES POLICY

Approved by School Council –June 2018

RATIONALE

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

CORE EXPECTATION

Bentleigh Secondary College is committed to providing a computer network and digital resources that 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.

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

GUIDELINES

A STUDENT AT BENTLEIGH SECONDARY COLLEGE WILL BE RESPONSIBLE FOR:

BEHAVIOURS

1. Protecting one's own privacy rights and those of other students by not giving out personal details such as: full names, telephone numbers, addresses and images (this includes personal details, school details, images or photos).
2. Recognising other users' intellectual property and acknowledging these sources (in a bibliography including all text, images, and multimedia) where used.
3. Not participating in cyber bullying practices. In particular, students should not read or forward material that may be interpreted by others as bullying material and should report instances and material to a teacher. Students are expected to show exemplary behaviour in relation to any Cyber bullying, in line with DET Anti-bullying Guidelines and Bullying Policy.
4. Seeking teacher or parent advice if unsure regarding internet content or search methods, hostile or unpleasant emails, blogging or wiki content.
5. Avoiding all potentially offensive sites and refusing to be guided to these sites.
6. Ensuring that external data storage devices do not contain any programs or files that may cause harm or contain offensive material.
7. Respecting the rights of others in all collaborative, online communication forums, and email by using language that is polite and professional.
8. Respecting computer network security and the data of other users (including individuals, the college and the Department) and only log in using their own login code and password.
9. Ensuring that regular backup of data on an external hard drive is part of the procedure.

ONLINE ETIQUETTE (MANNERS)

This applies to all online digital interactions.

10. As online manners are very important, students must behave in a polite and fair manner at all times. Your words may be easily misunderstood or misinterpreted, so be considerate and tactful. You are never anonymous online. You are accountable. Your actions can be traced.
11. Respect the rights of others in all collaborative, online communication forums and email by using language which is polite and professional.

DOWNLOADING AND UPLOADING

This applies to downloading and uploading:

12. You are responsible for the material you download. If you download offensive material you may have to face the consequences of your actions. 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.
13. 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.
14. If a site has been blocked and you consider this site to be of educational benefit—inform your teacher. Do not bypass department/college network security to access games, music or social networking sites whilst at school.
15. Do not download blocked content at home and access them from your hard drive whilst at school.
16. The Australian Law and Digital Rights Management (DRM) states that it is illegal to download or share copyrighted music, video,

film and games without paying for them. Downloading these files illegally or sharing illegal downloads is breaking the law and you may be prosecuted.

USE OF EMAIL AND SECURITY

This applies to the use of email:

17. When emailing: imagine that you are speaking to the person and type a polite version of what you would say. Capitals are considered yelling.
18. 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.
19. Take care with your email account. Don't give out your email address to unreliable sites or your inbox may fill with SPAM (junk email—advertising).
20. Users must only send emails from their own named accounts. If you create an anonymous email account (i.e. Ilikered@gmail.com account) and send inappropriate emails from this account you can be tracked. Anonymous emailing such as this is prohibited.
21. Do not open emails that request that you update certain programs such as 'Flash' or 'iTunes'. Requests to update will generate from the programs themselves and will never be emailed. Do not open emails that promise gifts and opportunities. Simply opening these emails (not even the attachments) can release viruses or Trojans into your computer.
22. Students must not use their digital device or college owned devices to create, save or send messages that contain offensive language, graphics, images – including photographs or film, 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 college community is involved in sending such an email, or communicating such information using the Internet (whether from inside the college or beyond it) it is considered a breach of the ICT Policies.
23. Email accounts are not designed for storing information. You need to save important information as documents on your hard drive. Your Bentleigh/O365 account may delete emails automatically after 30 days. Clean out your deleted messages and sent mailboxes every fortnight.

PROCEDURES for BREACHES to the AGREEMENTS and POLICIES

The college will be vigilant in managing student use of the resources to improve learning outcomes. Misuse of desktop computers, laptops, notebooks, tablets, digital cameras and other technologies and mobile ICT devices will be dealt with according to the nature of the infringement.

Breaching the conditions stated in the Ethical and Responsible Use of Digital Technologies Policy and the ICT Acceptable Use Policy may result in access restrictions and/or withdrawal of access to digital resources.

Ongoing Monitoring

The college reserves the right to remotely and locally monitor student and college based devices on an ongoing basis. Students found to be breaching the conditions of the ICT Policies will be issued consequences. Students may be called up at any time by ICT, Sub-School or Principal Class staff to have their device checked for compliance with the college ICT Policies.

MAJOR BREACHES

The following are considered major breaches:

1. Endangering the health and safety of or the property of others;
2. Vandalising the property of others;
3. Harassing or bullying others;
4. Persistent minor breaches;
5. Accessing blocked sites using VPNs, altering DNS settings to bypass the college proxy server, or accessing the internet by tethering to smart devices or internet dongles with the intent of bypassing the college monitoring systems and filters;
6. Downloading, displaying, saving, or transmitting any material that others may find offensive. This includes violent, racist, sexist material and pornography;
7. Bypassing filters and network security with the intention of changing settings and or interfering with existing sites;
8. Using someone else's password to access email, intranet profiles or other online forums under their identity;
9. Knowing about and failing to report or encouraging any of the above infringements to a teacher/coordinator or member of the Principal team.

Procedures and consequences for major 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;
- Temporary confiscation of the device/s (including, but not limited to, computers or other mobile ICT devices);
- Removal of email privileges and/or internet and network access;
- If equipment and/or notebook is damaged, where the device is owned by the college, 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.

MINOR BREACHES

The following are considered minor breaches of the policy guidelines:

1. Playing games;
2. Straying to sites irrelevant to 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 notebook;
6. Changing settings for virus protection, spam and filtering that have been set as a departmental or school standard.

Procedures and consequences for minor breaches:

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 breaches, the student will be sent to an Assistant Principal or the Head of Sub School. The student and teacher will complete an incident report. Students will incur one or more of the above consequences at the discretion of the teacher, Head of Sub School and/or Assistant Principal.

Digital acceptance of this Policy is required via the payment portal for the Managed BYOD Program (2019-2021) through edunet and as part of the Bentleigh Secondary College online course confirmation via Compass.

EVALUATION

Review annually, by Policy and Accountability Committee with recommendations to College Council