ICT ACCEPTABLE USE POLICY

Approved by School Council – August 2016

RATIONALE

ALL students and their parents/guardians/caregivers at Bentleigh Secondary College must digitaly accept this agreement. This agreement covers the use of technologies that are beyond the One to One Notebook Program and include, but are not limited to, desktop computers, laptops, tablets, projectors, digital cameras, photocopiers, mobile phones, music storage devices and audio visual equipment.

GUIDELINES

A STUDENT AT BENTLEIGH SECONDARY COLLEGE WILL BE RESPONSIBLE FOR:

1. Ensuring mobile phones and other personal technologies are not seen nor used at college during the course of the school day, unless specifically instructed by a teacher.
2. Ensuring personal mobile phones/technologies are locked away safely and not left unsecured at any time. The college bears no responsibility for any personal technologies that are brought to school.
3. Understanding that the use of technologies in school is primarily to support learning.
4. Ensuring that games—online, installed, or on an external drive—and other recreational programs not directly linked to learning are not accessed during school hours. This includes video conferencing and instant messaging software such as Twitter, Skype, Facebook, and equivalents.
5. Not removing, or attempting to remove, any software installed by the college on the device.
6. Only accessing the Internet by using the college network when at school. Tethering to a smart device or Internet dongle is strictly prohibited; the bypassing of the Bentleigh proxy server to access blocked sites is prohibited. This includes using VPNs and the altering of DNS settings.
7. Understanding that 'Torrent' downloading is strictly prohibited at school.
8. Not accessing, or attempting to access, monitor or tamper with, information on any of the college servers or any other person or organisation's computer without explicit agreement of that person or organisation.
9. Downloading and running only authorised programs and learning games; and maintaining settings for virus protection, spam and filtering which the school and/or Department have set.
10. Ensuring that passwords are private and confidential, not shared with anyone, and changed regularly.
11. Understanding that all actions taken using the student's user account are the responsibility of the account owner and that the network account (username and password) identifies the student and that all communications (both external and internal) may be monitored.
12. Understanding that notebooks may be monitored during lessons and breaks to determine how students are using the device—consequences will follow for students found to be breaching the use agreement.
13. Complying with all legal requirements governing the use of the notebook and the accessing of information—such requirements include, but are not be limited to, privacy and intellectual property rights laws, and Identity Theft and copyright – this directly relates to item 10. Torrent downloading is strictly prohibited.
14. Ensuring that all schoolwork and other data is regularly backed-up. Weekly backing-up of school related work is encouraged. Only school related work can be backed-up on the student H: Drive on the Bentleigh Secondary College network. Students are encouraged to store personal data on an external device. The college is not responsible for the loss of any work or files from students' notebooks due to damage, hardware or software failure.
15. Not tampering or changing any anti-virus, security, monitoring or remote access settings on the notebook computer that have been set by the college.
16. Understanding that the college reserves the right to remotely install or make changes to existing software in network updates and students must not override these changes.

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, the ICT Acceptable Use Policy and the One to One Notebook Acceptable Use Agreement 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 Acceptable Use Agreements will be issued consequences in line with this policy. 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 Acceptable Use Agreement.

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, 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.

EVALUATION

Review annually, with recommended changes being presented to College Council