Bentleigh Secondary College

ICT Acceptable Use Policy

Rationale

ALL students and their parents/guardians/caregivers at Bentleigh Secondary College must digitally accept this agreement.

This agreement covers the use of Personal and learning Technologies at Bentleigh Secondary College. We define Personal Technologies as, but are not limited to, laptops, tablets, digital cameras, mobile phones, communication devices and music storage devices. Technologies also encompass desktop computers, projectors, photocopiers devices and audio-visual equipment.

Guidelines

A student at Bentleigh Secondary College will be responsible for:

- Ensuring mobile phones and other personal technologies are not seen nor used at college during class time or during breaks, unless specifically instructed by a teacher.
- 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.
- Understanding that the use of technologies in school is to support learning.
- 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 social media, video conferencing, and instant messaging software such as Teams, WhatsApp, Facebook, Instagram, Tiktok and equivalents.
- Not removing, or attempting to remove, any software installed by the college on all digital technologies without permission or instruction to do so.
- Only accessing the Internet by using the college network when at school. Tethering to a smart device or internet dongle is strictly prohibited unless for educational purposes approved by a teacher; the bypassing of the Bentleigh proxy server to access blocked sites is prohibited. This includes using VPNs and the altering of DNS settings.
- Understanding that 'Torrent' downloading is strictly prohibited at school. Complying with all legal requirements governing the use of the notebook and the accessing of information—such requirements include, but are not limited to, privacy and intellectual property rights laws, and identity theft and copyright.
- Not accessing, or attempting to access, monitor or tamper with, information on any of the college servers or any other person's or organisation's computer without explicit agreement of that person or organisation.
- 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.
- Ensuring that passwords are private and confidential, not shared with anyone, and changed regularly.
- 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.
- Internet usage and Personal Technologies 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.
- Ensuring that all schoolwork and other data is regularly backed-up. Weekly backing-up of school related work is encouraged. 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.
- Not tampering or changing any anti-virus, security, monitoring, or remote access settings on the notebook computer that have been set by the college.
- Understanding that the college reserves the right to remotely install or make changes to existing software.
- Not using their Personal Technologies 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 or strong reaction). Whenever a member of the college community is involved in sending an email or communicating such information using the Internet (whether from inside the college or beyond it) it is considered a breach of ICT Policies. In the event that a class needs to have access to mobile phones for

data recording or for folio record keeping or for other appropriate school learning, a Compass event is to be created and signed by the parent / carer before the device is brought to and used in class.
- No filming / taking photos of anyone unless explicit consent has been sought
- No charging onsite – arrive with a fully changed computer. This is an OHS requirement of the school. In an emergency (computer required for Assessment) the computer may be taken to IT at the appropriate break where it can be charged for that break. Please note, IT may not have the appropriate charger for all BYOD devices, in which case, no assistance can be offered.

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 Digital Technology 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, while onsite, and locally monitor student owned and college-based devices on an ongoing basis. Students found to be breaching the conditions of 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. Internet traffic is audited regularly and breaches are investigated to ensure the safety and wellbeing of everyone in the BSC learning community.

Major Breaches

The following are considered major breaches:
- Endangering the health and safety of or the property of others
- Vandalising the property of others
- Harassing or bullying others
- Persistent minor breaches
- 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
- Downloading, displaying, saving, or transmitting any material that others may find offensive. This includes violent, racist, sexist material and pornography
- Bypassing filters and network security with the intention of changing settings and or interfering with existing sites
- Using someone else's password to access email, intranet profiles or other online forums under their identity
- 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 consquences imposed:
- Temporary ban on Personal Technologies
- 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 Personal Technology 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
- Authorities such as police may be contacted where the law has been breached
- Education with the student around the area of concern

Minor Breaches
The following are considered minor breaches of the policy guidelines:

- Playing educational or non-educational games during school times without permission to do so.
- Filming or photographing members of the school community, unless for an educational activity without permission or consent to do so.
- Misuse of the internet during school hours' time – no games on site during breaks and before / after school
- Communicating digitally when not relevant to the requirements of the learning task.
- Disseminating irrelevant material.
- Failing to follow fair and reasonable instructions – such as not ceasing to use or put away the Personal Technologies when required.
- 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 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 of the Bentleigh Secondary College online course confirmation via Compass.

Policy Review and Approval

Policy last reviewed	2024
Ratified by	School Council
Next scheduled review date	2027