

## ICT POLICY

Our students are living in an increasingly technological world. At Beaumaris Secondary College, we support the right of all members of the school community to access safe and inclusive learning environments, including digital and online spaces. This form outlines the School's roles and responsibilities in supporting safe digital learning, as well as the expected behaviours we have of our students when using digital or online spaces.

At our School we:

- Have a **Student Engagement Policy** that outlines our School's values and expected standards of student conduct, including consequences for breaching the standards. This Policy extends to online conduct which includes:
  - Programs that educate and model safe and responsible use of digital technologies to our students.
  - Information about digital access issues such as online privacy, intellectual property and copyright;
  - Supervision and support students using digital technologies in the classroom;
  - Protocols and procedures to protect students working in online spaces. This includes reviewing the safety and appropriateness of online tools and communities, and removing offensive content at earliest opportunity;
    - [Duty of Care and Supervision](#)  
([www.education.vic.gov.au/about/programs/bullystoppers/Pages/prindutycare.aspx](http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/prindutycare.aspx))
- Provide a filtered internet service to block inappropriate content. We acknowledge, however, that full protection from inappropriate content cannot be guaranteed
- Use online sites and digital tools that support students' learning;
- Address issues or incidents that have the potential to impact on the wellbeing of our students;
- Refer suspected illegal online acts to the relevant Law Enforcement authority for investigation;
- Support parents and care-givers to understand safe and responsible use of digital technologies and the strategies that can be implemented at home. The following resources provide current information from both the Department of Education & Training and The Children's eSafety Commission:
  - [Bullystoppers Parent Interactive Learning Modules](#)
  - [iParent | Office of the Children's eSafety Commissioner](#)
  - (<https://www.esafety.gov.au/education-resources/iparent>)

Staff will actively seek and utilise the use of Learning Technologies where it enhances the learning process. Staff are encouraged to utilise a range of digital literacies.

## **Objectives**

In utilizing ICT to engage and enhance learning, the College shall:

- a) Facilitate students in using a variety of ICT to aid their Thinking, Creating, Collaboration, Communication and Presentation.
- b) Provide a thorough educational plan that involves the use of ICT throughout the curriculum.
- c) Use Learning Technologies to motivate and engage students in their learning.
- d) Implement a program of staff professional development in the effective use of ICT.
- e) Encourage the use of regular staff communication via Microsoft Teams.
- f) Develop and publicise an 'acceptable use policy' for staff and students that is available to all members of the school community.
- g) Ensure that all staff are aware of DET policies regarding the use of ICT.

Beaumaris Secondary College works towards the purposeful integration of digital technologies throughout the curriculum. Staff at the college use a variety of ICT hardware and software in their lessons and extracurricular activities. The college provides regular professional development to ensure that staff are skilled up in using digital technologies to improve and enhance curriculum for the improvement of student outcomes.

Access to computers and computing resources is conditional and includes access to such things as user folders, your email accounts, the internet and intranet at school. All computing resources are provided as an educational tool to support learning.

## **Passwords and network access**

- 1.1 Students are allocated a USER NAME and PASSWORD.
- 1.2 Students will use Office 365 to access resources, complete tasks, collaborate on projects, share and submit learning.
- 1.3 All students will be given a school email account.
- 1.4 Passwords and usernames are not to be shared.
- 1.5 Students should go to the Genius Bar(IT Support-located on Ground level) immediately if they believe that other people know their user name and/or password or if they detect any unauthorised activity with their account and reset their password.
- 1.6 Students using passwords in the collaboration space of Office 365 must share the password with the teacher so it can be moderated.
- 1.7 Unnecessary files in home drives should be deleted
- 1.8 Students must not place any offensive or illegal material on the college network.

## **Using software and accessing the college's network**

### **1.9 Loading Software**

- 1.9.1 The system administrator (SA) is authorised to load software onto student devices that are used for teaching and learning purposes.
- 1.9.2 Any student detecting a virus, or what they believe may be a virus, should contact the SA immediately.
- 1.9.3 No student is to tamper with any virus detection or prevention software in place on devices.

### **1.10 Internet access**

- 1.10.1 Internet access is provided for educational purposes only.
- 1.10.2 The college has deliberately limited internet access through a range of measures to ensure that the content accessed by students is appropriate, safe and monitored.
- 1.10.3 Students are not permitted to by-pass safeguards and any attempt to do so will result in students being disciplined appropriately.
- 1.10.4 The use of any software or web sites designed to deliberately by-pass the college's internet management systems is strictly prohibited. If this occurs students will be disciplined appropriately.
- 1.10.5 Access to sites not related to specific subjects or curriculum being studied are prohibited at school unless approved by the SA and E-Learning Group (ELG).

#### **Observing copyright**

- 1.10.6 Commercial music/video/text or other copyrighted material must not be stored on the college network or devices.
- 1.10.7 Students should not use the college resources to copy, duplicate, or modify the content of commercial electronic media.

#### **Plagiarism**

- 1.10.8 Students must not plagiarise the work of others.
- 1.10.9 Information sourced from the Internet must never be falsely passed on as one's own work.
- 1.10.10 Where information is copied directly from another writer or site the appropriate acknowledgement must be given to the original source.

#### **Offensive or inappropriate content**

- 1.10.11 In the event of offensive or inappropriate material being accessed or stored on a College computer, a report should be made to the SA.
- 1.10.12 If a student detects the material, then they should inform their mentor or teacher.
- 1.10.13 Any person found to be publishing or distributing inappropriate material will be subject to the Student Engagement and Wellbeing Policy.

#### **Using school email, Office 365 and social networks.**

- 1.10.14 Student school email, Office 365 and Compass are to be used to share educational material.
- 1.10.15 Students should not share personal information (telephone number, address etc.) by email or publicly viewable websites.
- 1.10.16 Students must not impersonate a teacher or create personal social groups
- 1.10.17 All communication should be polite and respectful at all times.
- 1.10.18 The use of obscene, offensive, disrespectful or aggressive language towards others is unacceptable over an electronic communications medium and Student Engagement and Wellbeing Policies will be applied accordingly.
- 1.10.19 Students must not use online communication tools to prepare or send unsolicited commercial correspondence. The college communications

systems (email, chat, sms) is not to be used for any commercial or business purposes (buying, selling and online banking).

- 1.10.20 Students must not use online communication tools to harass or annoy other users or for repeatedly sending unsolicited email to any users.
- 1.10.21 Students must report online bullying and harassment to school staff so it can be followed up and resolved.
- 1.10.22 Using social networks at school such as Facebook, Instagram and Snapchat is not appropriate for school use unless directly authorised by a teacher.

### **Phones Devices - Mobile Phones, Smart Phones and Communications Devices**

- 1.10.23 Phones are permitted at school under certain conditions.
- 1.10.24 Phones should be kept in lockers during school hours. School expects students to be off their phones once on school grounds. Phones are not permitted for excursions or camps unless otherwise stated by the school. Phones can be confiscated by teachers if used during school hours or on school grounds.
- 1.10.25 If inappropriate mobile use is seen by teachers, students will be subject to the Student Engagement and Wellbeing Policy.
- 1.10.26 Teachers may request or allow students to use a device for a specific task such as making a call to an INNOVATE Expert as part of a project.

### **1.11 Student Personal Computing Devices for teaching and learning purposes**

- 1.11.1 The primary student device is expected to be brought to school each day ready with applications appropriate for learning.
- 1.11.2 The primary device's base standards are set by the ELG each year.
- 1.11.3 Devices are expected to be brought to school fully charged ready for learning each day.
- 1.11.4 The primary device is a learning device and should be ready at all times for school work.
- 1.11.5 Students should never leave any device unattended at any time.
- 1.11.6 When not in use the device should be stored in the student's locked locker.
- 1.11.7 Devices can be inspected at any time upon request by teachers for inappropriate material.
- 1.11.8 Students will not operate any computing device that belongs to another student or staff member without their expressed permission.
- 1.11.9 Teachers may ask students to use mobiles in class. This is at the teacher's discretion within the learning context of the class.

### **Genius Bar**

- 1.11.10 A signed note from home must be brought to GOAL mentors in order for the student to borrow a school device.
- 1.11.11 The school kiosk devices may be borrowed by students in emergency situations only.
  - 1.11.11..1 A device is lost or has been stolen
  - 1.11.11..2 A device is damaged & being repaired
  - 1.11.11..3 A device is on order.
- 1.11.12 These devices are NOT for loan by students who have forgotten their device.

## **Device access by staff**

1.12 Any BYOD device a student brings to school may be accessed by the SA in the course of assisting with setting up devices or monitoring on the school network.

## **Privacy**

1.13 Teachers are able to see into student folders.

1.14 Students are never to photograph, video record or sound record another student or teacher without permission.

1.15 Students are never to publish over the Internet photographs, video recordings or sound recordings of teachers without permission from those in the media.

1.16 Students are responsible for the contents of their folders. Should they detect any content that they did not place there, or that does not belong to them, they should contact the Genius Bar.

## **STAFF COMPUTER ACCEPTABLE USE POLICY**

Beaumaris Secondary College will use digital technologies to prepare students to be critical online citizens with strong digital literacy skills. Staff will provide engaging and relevant curriculum that integrates digital technologies. The College offers Professional Development to ensure that staff are skilled in using digital technologies to improve student learning.

The purpose of this policy is to introduce the procedures and policies that the College has in place to ensure that the users of the College's ICT equipment are familiar with the protocols in place for the use of this equipment.

### **Hardware Management**

#### **1) Equipment Configuration (College Desktop computers)**

Users of Learning Technologies equipment are not permitted to alter the configuration of the College desktop computers without the approval of the EWG. This means that staff should not add or remove icons to the desktop or alter the 'Control Panel' without permission.

#### **2) Movement of hardware**

Hardware may only be moved or relocated at the direction of the EWG. No hardware may be removed from the College premises without the prior approval of the Principal or an AP.

#### **3) Correct use of hardware**

If you are using hardware with which you are not familiar, seek instructions from the Genius Bar. This applies to computers, photocopiers, digital cameras, video cameras etc.

### **Software Management: Loading Software**

The Genius Bar Technicians are the only people authorised to load software onto a desktop computer at the College. In the case of your DET notebook, it is the responsibility of each staff member to ensure that no licence breach will result from the software they load onto their DET notebooks.

Any person detecting a virus, or what they believe may be a virus, should contact the ICT Department immediately. They will coordinate the shutting down of the network, decontamination and rebooting

of the network (if necessary). No person is to tamper with any virus detection or prevention software in place on College equipment.

Each staff member at the College is allocated a USER NAME and PASSWORD. They are also allocated a FOLDER to store files and a SUBMIT folder, where students can deposit completed work that has been set by you.

**It is the responsibility of each network user to ensure that:**

1. They do not place, or allow to be placed, any offensive material on the College system.
2. Passwords/User Names are kept secret and not divulged to anyone. See the ICT Department IMMEDIATELY if you believe that other people know your user name and/or password or you detect any unauthorised activity with your account.
3. Folders are regularly maintained and unnecessary files deleted.

**Internet**

1) Staff access to the Internet is governed by DET guidelines. The acceptable use of the internet/email can be viewed at:

<http://www.education.vic.gov.au/about/deptpolicies/acceptableuse.htm>

2) Inappropriate Material

Inappropriate material is ANYTHING that makes the person who is viewing it feel uncomfortable. This also applies to material that violates copyright regulations (music, film, text etc.) or material that is not in keeping with the educational nature of the system.

Commercial music/video/text or other copyrighted material should not be stored on the College network.

Breaches of the DET policy may result in disciplinary action including revoking or restricting any right to use Electronic Communications, cautioning, or, in appropriate circumstances, may lead to more serious disciplinary action including termination of employment and possible reporting to the police.

3) Use of e-mail

Staff use of email in sharing information with colleagues, interacting with students and communicating with each other is encouraged and Professional Development in its use is provided regularly through the PD Program.

The acceptable use of electronic communications is covered by the DET policy above.

**Student declaration**

When I use digital technologies and the internet I agree to be a safe, responsible and an ethical user at all times by:

- Respecting others and communicating with them in a supportive manner;
- Never participating in online bullying (e.g. forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviours);
- Protecting my privacy by not giving out personal details, including my full name, telephone number, address, passwords and images;
- Protecting the privacy of others by never posting or forwarding their personal details or

images without their consent;

- Talking to a teacher or a trusted adult if I personally feel uncomfortable or unsafe online, or if I see others participating in unsafe, inappropriate or hurtful online behavior;
- Thinking carefully about the content I upload or post online, knowing that this is a personal reflection of who I am and can influence what people think of me;
- Reviewing the terms and conditions of use for any digital or online tool (e.g. age restrictions, parental consent requirements), and if my understanding is unclear seeking further explanation from a trusted adult;
- Meeting the stated terms and conditions for any digital or online tool, and completing the required registration processes;
- Handling ICT devices with care and notifying a teacher of any damage or attention required;
- Abiding by copyright and intellectual property regulations by requesting permission to use images, text, audio and video, and attributing references appropriately;
- Not accessing media that falls outside the School's policies;
- Not downloading unauthorised programs, including games;
- Not interfering with network systems and security or the data of another user;
- Nor attempting to log into the network with a user name or password of another student.

In addition, when I use my personal mobile phone I agree to be a safe, responsible and ethical user at all times, by:

- Keeping my device in my locker during school times;
- Only taking and sharing photographs or sound or video recordings when others are aware the recording is taking place and have provided their formal consent as part of an approved lesson.

---

### **Agreement signatures**

Students and parents are required to complete an Acceptable Use Agreement upon enrolment.