ICT: Acceptable Use Agreement (AUA)

Rationale:

At Kambrya 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 policy 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.

Aim:

The Acceptable Use Agreement (AUA) describes the programs and processes a school has in place to support students to be safe, ethical, and responsible users of digital technologies. For Department of Education and Training (DET) or school-owned digital devices and technologies lent to students for use at home, that use must be for educational purposes only.

The AUA outlines the expected behaviour of students and seeks informed understanding and agreement.

The policy applies to use of ICT at Kambrya College or student participation through DET endorsed learning agencies- Virtual Schools Victoria (VSV) or Victorian School of Languages (VSL).

Definitions

For the purpose of this policy, Information & Communication Technologies (ICT) are defined as being any electronic devices or applications which allows a user to access, receive, record, copy or send information as text, images, audio, or video.

ICT includes, but is not limited to:

− Computer systems and applications such as email, and the internet
− Networks
− Electronic storage devices
− Mobile devices such as mobile phones, tablet devices and PDAs
− Web-based tools: e.g.- social networking sites, chat rooms, blogs, podcasts, instant messaging and file sharing.
− Imaging tools such as video, still or web cameras and related software
− Audio tools such as audio recording devices, mp3 players and related software
− Fax and copying machines

Implementation

- Staff use of Kambrya College's devices and/or network to access the internet or any other ICT application, is governed by the Department's overarching policies, which are amended from time to time

- Kambrya is committed to safely and responsibly using digital technologies as an integral component of the learning and teaching programs. Student use of our devices and/or network to access the internet or any other ICT application is governed by this policy; reinforced by the *ICT- Acceptable Use Agreement form* (Attachment A).

- Students will be made aware of behaviour which is not acceptable when using ICT and the school's Student Engagement - Discipline Policy will apply to breaches of expected behaviours.

- Staff and student personal ICT devices should be stored in a safe and secure place as the school will not be held liable for loss, damage or theft.

- Distribution of school owned devices to students and personal student use of the internet at school will only be permitted where students and their parents/carers provide written acknowledgement that students agree to act in accordance with the conditions of loan and standards of conduct.

- The Department's *Acceptable Use Policy for ICT Resources* **(2020)** applies to all school staff, who need to familiarise themselves with the content of that policy. Breaches of this policy may result in disciplinary action.

- Cameras, still and video (including mobile phone cameras) must not be used in private spaces, for example; changing rooms, toilets, gyms and swimming areas. Action will be taken against any student or staff member who photographs or films other individuals without their knowledge or permission.

    - Photographs, video or digital images of a student are considered "personal information" and therefore their use and disclosure are governed by the *Privacy and Data Protection (PDP) Act 2014* (Vic) and the Information Privacy Principles contained within it. Photographs, video and digital images of students may also contain copyright, and therefore may also be governed by the Copyright Act 1968 (Cth). To comply with the PDP Act, Kambrya College will gain parental consent before collecting, using, sharing or displaying student photographs and film internally or on its social media / College webpage.

- Kambrya College will exercise special care and diligence when photographing & filming Aboriginal and Torres Strait Islander individuals and communities. Premised on mutual respect, trust and the principle of free, prior, & informed consent, the following will be discussed with the appropriate custodian/s prior to taking any footage:
    - A clear explanation of the film or photo process
    - Proper information about the project, including the message, the medium and the audience
    - All proposed and foreseeable uses of the material, including secondary uses
    - The impacts of the material being disseminated
    - Timeframes
    - Any relevant intellectual property matters
    - That the person can choose not to be photographed or filmed.

    Teachers and staff must not use any materials for purposes or uses other than that for which individuals have provided their free, prior and informed consent. Images should also be positive and empowered images to assist in the promotion of the rights of Aboriginal and Torres Strait Islander peoples. As with all students, written consent is required for the photographing or filming of any student of Aboriginal or Torres Strait Islander background.

Responsibilities and Consequences

The use of the Kambrya's ICT resources, including network, is subject to the Acceptable Use Agreement Policy (for staff and students). The school's ICT resources can only be used for or in connection with the educational or administrative functions of the school or participation in an alternate learning environment; such as- Virtual Schools Victoria (VSV) or the Victorian School Of Languages (VSL).

Network

No student is permitted access to an IT classroom unless under the direct supervision of a teacher, who must remain in the room at all times. Similarly, no student is permitted to remain in the room after class unless the teacher remains in the room to supervise the student.

Students **must no**t:

- Remove, damage or attempt to repair any component of the Network.
- Bring or consume food or drink in a computer room or pod.
- Through direct action cause damage to the computer network.
- Download and Install any software onto the college's computer hardware.
- Attempt to access secured parts of the network.

- Connect non Kambrya College hardware to the ICT network without permission from the IT Department. This excludes student BYOD and leased devices.
- Use another user's account including students and teachers to access the computer network.

Students **must**:

- Immediately report any and all problems with the College, VSV or VSL Computer Network to the classroom teacher.
- Demonstrate appropriate respect for property.
- Use only those applications that apply directly to current work.
- Ensure that any removable media device used on the network is virus free.
- Leave the computer room of pod in a tidy state
- Ensure all computers are logged off, shutdown and that the area around their workstation is tidy.

All users have a responsibility to:

- Report any faults.
- Not disclose their password or logon details, except to the College IT Technicians, if requested.
- Lock their workstation if leaving it unattended.
- Use the computer network only for work that is directly related to education or educational purposes.
- Abide by copyright and licencing laws
- Ensure all data is backed up on a regular basis. The college is not responsible for any loss or corruption of data.

The **College / VSV / VSL Internet facilities must not** be used to:

- Access, view, download, print, disseminate or post any material that may be considered inappropriate, offensive, defamatory, obscene, pornographic or discriminatory, including material that is sexually explicit or that has racist, sexist, discriminatory, political or religious content, or which includes inappropriate comments in relation to sexual orientation, disabilities or any other physical attributes. *This list is not exhaustive*.
- Attempt to probe security mechanisms at the College, other educational institutions, or any internet sites.
- Post any information on Internet news groups, bulletin boards or similar forums on behalf of the College unless specifically authorised to do so.

During the course of a **network Internet session, students must not:**

- Download any program except under the explicit instruction of the classroom teacher.
- Play online games.
- Access any streaming media, except under the explicit instruction of the classroom teacher.
- Knowingly download a virus or similar program that will cause damage to the computer network.

Users of the **College's e-mail system must not** use it:

- In a way that may be considered offensive, defamatory, obscene, pornographic, discriminatory, insulting or disruptive to any other person (for example, pictures of naked people, semi clothed people, personal comments about colleagues, students or staff).

- To access, view, download, print or send messages or attachments (including to home e-mail), which include:
  - Language that is not appropriate including, but not limited to, swearing, sexually explicit references.
  - Sexually explicit messages or pictures.
  - Offensive or inappropriate cartoons or jokes.
  - Unwelcome propositions or love letters.
  - Ethnic or racial slurs.
  - Content that would deemed discriminatory.

- To access other people's e-mail accounts.

- For sending chain mail, gambling, participating in on-line games, retrieving games or screen savers unless there is a business need to do so, joining a mailing list or chat group, posting messages to news groups, or engaging in on-line purchasing or selling.
- To distribute the copyright material of third parties, including software, database files, documentation, pictures, articles, graphic files, text or other downloaded information.
- For intentional dissemination of any computer viruses.
- For personal advertising or for personal profit making.
- For distributing personal information (information or an opinion that can identify a person) about a person unless the person's consent is obtained.

The College understands that computer users cannot always control the messages that are sent to them. However, computer users must discourage third parties (such as family, friends or workmates) from sending inappropriate messages to them.

If a computer user receives an inappropriate message or attachment to an e-mail the user must:
- Inform the ICT Technicians and a Principal Class member.
- Delete the e-mail.

All **Acceptable Use** terms and conditions apply to users who connect to the network or access the Internet using a laptop computer.

All supplied laptop computers remain the property of the College and as such the use of these machines are bound by the Information and Communication Technology Policy.

Removable media

The College understands that removable media is necessary for use with computer data transfer and storage. As they are attached to the computer network, the following rules apply.

Users must:
- Ensure that all files are free of viruses.
- Accept responsibility for the maintenance of the device.

Users must not:
- Download inappropriate material to any removable media device as stated in the network, Internet and e-mail sections.
- Use the device for the storage of material that is prohibited by the *ICT- Acceptable Use Agreement Policy.*
- Use the device for accessing prohibited material.

BREACHES OF ICT POLICY

Consistent with the *Student Engagement - Discipline Policy,* breaches of the *ICT- Acceptable Use Agreement Policy* by students and staff can result in a number of consequences depending on the severity of the breach and the context of incident.

For Students;
- Removal of network access privileges.
- Removal of email privileges.
- Removal of internet access privileges.
- Removal of printing privileges.
- Indefinite ban.
- Payment for repairs.
- Conference with parents.
- Other disciplinary action as determined by the Principal or Assistant Principal. Activity which may be deemed to be criminal will be reported to the police for investigation.

For Staff:

Non-compliance with the Acceptable Use Policy will be regarded as a serious matter and appropriate disciplinary action may be taken.

Use of ICT to engage in behaviour that amounts to bullying, harassment or unlawful discrimination is prohibited and may result in disciplinary action.

While the internet may be largely a self-regulated environment, principles of defamation law, privacy law and community standards still apply to communication and publishing via the internet or other electronic means. In addition to school consequences, there are legal sanctions for improper use of the internet and ICT.

Service warranty

The College makes no warranties of any kind, whether expressed or implied, for the service it is providing. The College will not be responsible for any damage a user suffers. This includes, but is not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, data corruption, or service interruptions caused by Kambrya College, or the ISP. Use of any information obtained via the Internet is at the user's own risk. The College specifically denies any responsibility for the accuracy or quality of information obtained through its services. All users need to consider the source of any information and consider how valid that information may be (reliability of source, accuracy, timeliness, completeness, etc).

College Leased Laptops

From 2021, Kambrya College will lease a number of its laptops to students, under agreement. The laptops remain the property of the College and students must not intentionally damage or misuse the device in any manner or use the laptop contrary to the Network, Internet, or Email sections of this Policy.

STUDENT DEVICE USAGE GUIDELINES

Introduction:

To enhance the learning experience of its students, Kambrya College aims to provide student's access to its Wireless Network and the option of utilising various devices. The purpose of these guidelines is to ensure that students and their parents recognise the limitations that the College imposes on the use of personally owned and leased devices when they are used at the College in conjunction with the wireless network.

In the event that the College forms a reasonable belief that a personal mobile device contains illegal content or evidence that may be required by police in the course of any investigation, the mobile device will be confiscated and held until such time that further advice has been sought from police regarding the content.

COLLEGE GUIDELINES ON PERSONAL DEVICES

Students are expected to:

1 Be responsible for leased, school provided or their own devices (and their use), at all times. Devices must be kept in a <u>locked</u> locker when not in use. The College will not be held responsible for any damage, loss or theft of any student device.

2 Be responsible and liable for any damage that they may cause with their device.

3 Use devices in the classroom at the discretion of the classroom teacher. Classroom teachers may prohibit, restrict or regulate use of devices as they deem necessary.

4 Charge the batteries of their device overnight and bring a fully charged device to school. Students may access the College 'laptop charging stations', as per school protocol.

5 Use their device to support the classroom activities and educational aims of the College.

6 Carry their devices in padded bags or hard cover cases when moving between classrooms and to and from school to prevent damage to the device.

7 Use their devices *only* for study purposes and in supervised areas such as the Library and Study Areas during these times: before school, during recess, at lunch and after school.

8 Install a reliable and updated anti-virus program to protect their devices, and the College network from contamination by computer viruses.

9 Accept that College Staff have the right to inspect the device and its contents to ensure compliance with this policy.

10 Ensure all data is backed up on a regular basis.

Students are NOT Permitted to: During class time or whilst on camp or excursion

1 Play games, access social media or take part in any other activities that are not related to their learning in class time except under the explicit instruction of the classroom teacher.

2 Use their devices to cause distraction for others, especially in regard to sound. Therefore, audio must be muted at all times or restricted with student owned headphones or earphones when directed by the teacher.

3 Use their device to listen to music during class time unless curriculum related and under the explicit instruction of the classroom teacher.

4 Film or record any student or staff member using the camera or microphone in the devices without the express written permission of the College AND the individual concerned.

5 Take photos of themselves or others and upload them on ANY social media websites.

6 Avoid/Bypass the limitations set by the College network, particularly Internet restrictions through mobile network devices or phone hotspots while on College premises.

7 Share passwords or any other access codes with any other person or use another user's account to access the computer network.

8 Use the devices for SAC/SAT school-based examinations, unless notified by your Teacher.

The College ICT Department will provide assistance with connection to the College network, but will not be responsible for, nor be required to provide, any support or troubleshooting of any issues.

Usage Consequences

Failure to comply with these guidelines and policies may result in disciplinary action by the school which may include, but is not limited to, loss of access to the Kambrya College ICT Network.

Resources for Parents

The following resources provide current information from both the Department of Education and Training and The Children's eSafety Commission:

-   Bullystoppers Parent Interactive Learning Modules
    (www.education.vic.gov.au/about/programs/bullystoppers/Pages/parentmodules.aspx)

-   iParent | Office of the Children's eSafety Commissioner
    (https://www.esafety.gov.au/education-resources/iparent)

References:

https://www.education.vic.gov.au/school/principals/spag/governance/Pages/privacy.aspx

Evaluation:

This policy will be reviewed as part of the school's three-year review cycle.

Author	Keith Perry- College Principal and Chris Outhred- ICT Manager
Approved by Kambrya College School Council	August 2020
Responsible for Review	Paul Looker- Assistant Principal and Chris Outhred- ICT Manager
Next Review Date	August 2021

KAMBRYA COLLEGE

(ICT) Acceptable User Agreement- <u>STUDENTS</u>

At Kambrya, 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.

The ***ICT- Acceptable Use Agreement*** (AUA) outlines the expected behaviour of students and seeks informed understanding. The agreement applies to use of ICT at Kambrya College or student participation through DET endorsed learning agencies- Virtual Schools Victoria (VSV) or Victorian School of Languages (VSL).

<u>At our School we:</u>

- Have a *Student Engagement Policy* and *ICT- Acceptable Use Agreement Policy* that outline our values and expected standards of student conduct, including consequences for breaching the standards.
- Have programs in place to educate our students to be safe and responsible users of digital technologies.
- Provide information about digital access issues such as online privacy, intellectual property, and copyright;
- Supervise and support students using digital technologies for school-directed learning;
- Use clear protocols and procedures to protect students working in online spaces. This includes reviewing the safety and appropriateness of online tools and communities, removing offensive content at earliest opportunity, and other measures;
- 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 caregivers to understand safe and responsible use of digital technologies and the strategies that can be implemented at home.

<u>Student declaration:</u>

When I use digital technologies & the internet, I agree to be a safe, responsible, and 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;
- Only taking and sharing photographs or sound or video recordings when others are aware the recording is taking place and have provided their explicit consent as part of an approved lesson and in line with the College *Student Mobile Phone Use* Policy;

- 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 behaviour;

- 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;

- Protecting the privacy and security of my school community / wider school learning community by not sharing or posting the link to a video conferencing meeting with others, offline in public communications or online on public websites or social media forums;

- 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;

- Not attempting to log into the network or online service with a username or password of another person.

This Acceptable ICT User Agreement form must be signed and returned to the College before a student will have access to ICT Technologies and Online Services at Kambrya College. Any questions should be addressed to the College and clarification obtained before the Agreement is signed.

By signing below, the Parent/Carer has read and explained the Kambrya College Acceptable ICT User Agreement carefully to the Student and together understands the significance of the terms and conditions and agrees to abide by them.

The Parent/Carer and Student agrees that Kambrya College reserves the right to make amendments to this agreement at any time. The College also reserves the right to default or suspend access to ICT resources should there be a significant breach to the terms and conditions set out in this agreement.

The Parent/Carer consents to the following been made available on the College's Online Services:

- Authorise permission for your child & parent/carer to access Compass School Manager & Microsoft Office 365.

- Allow personal information to be uploaded to these services as specified in this agreement, including the data being stored outside of Victoria.

- Enable the use of an individual's intellectual property as specified in this agreement.

Parent/Carer and Student Consent

Student Name: …………………………………………………....…   Year Level: ……………………………

Student Signature: ………………………………………………………   Date: …………………………….

Parent/Carer Name: …………………………………………………….…

Parent/Carer Signature: ………………………………………………………   Date: ……………………………..

Kambrya College Online Services

	Compass School Manager	Microsoft Office 365
Privacy Policy Link	http://compass.edu.au/policy/	http://office.microsoft.com/en-au/business/office-365-cloud-privacy-FX103046091.aspx
What does the online service provide?	This is the Online Learning Management System used by Kambrya College. This system provides Attendance, Student Management, Curriculum Resources, Room Resource Booking and Parent portal access.	Central online storage and collaboration service for staff and students of the college. Services offered include Email, SharePoint, OneDrive, Skype for Business, Microsoft Office, Sway, Yammer, Video, Office Mix and OneNote
Who is the Service Provider?	JDLF International Pty Ltd	Microsoft Corporation
What personal information of individuals will the school use and disclose to the service provider?	Students: • Full name • Contact information including: address, phone and email. • School • Student Management Information • Medical information (as provided by parent to ensure management of health issues) • Attendance information • Report information • Network user account information • Learning data • Curriculum data Parents: • Full name • Contact information including address, phone and email. • Parent Portal username and password information.	Students (Only): • Full name • Student Username • Year level • Email address (Username@kambryacollege.com) • School • Learning data • Curriculum data No health information or sensitive information will be disclosed to the service provider.
How will the school use the personal information of individuals?	**Students:** All data listed below will only be accessed by relevant staff members; • Full name and contact information: Made available so staff are able to contact relevant parties for various issues. • Student Management Data	Students (Only): • Student's personal information will be used to create an account in Office365. • Personal Data: Students personal drives will be hosted on the office 365 application (similar to a Dropbox setup).

	- Medical information: Alerts staff to medical issues. - Attendance information: Staff will collect attendance data and school will use such data to ensure that students are meeting college attendance requirements. - Report information: Reports will be uploaded to the site for parent/guardian access. - Network User information: Allows students to access the Compass School Manager. - Curriculum data: Any curriculum and assessment tasks may be hosted on Compass **Parents:** All data listed below will only be accessed by relevant staff members; - Full name and contact Information: Made available so staff are able to contact relevant parties for various issues. - Parent Portal username and password information: Used to access the Parent Portal on Compass School Manager.	Student work: Any student work completed in Office365 may be hosted in the Office365 service.
Where will the service provider store the personal information disclosed to it?	Various locations around Metropolitan Melbourne, Australia. This is also hosted within the Department of Education & Training ICT Network.	Storage locations for Microsoft Office 365 Education are: **Office 365 – Exchange Online, SharePoint Online, Skype for Business** - Melbourne – Australia Microsoft Datacentre - New South Wales – Australia Microsoft Datacentre - United States of America (USA) Authentication only, no personal data used (School Username and password)
What school policies apply to the use of these online services?	As per this policy and the school policies for: - ICT Acceptable Use Agreement (Computer use/internet use Policy); and - Student Engagement – Discipline	
Will the School be able to access and retrieve all content including messages or other communications from the online services?	All 3 applications have tools installed and service teams will allow the College to adequately track the usage and retrieve the data on these services.	

How will the service provider use personal information of individuals that is collected from the school?	Personal information provided will be used to create an account for students and parents, so they are able to access the services offered by COMPASS. Other Personal information provided will be used by Compass to provide Kambrya College with a School Management and Learning Management System. COMPASS School Manager does not share any information unless they have strict consent from Kambrya College. The college will not share any data to a 3rd party without the strict written consent of the parent and guardians of the concerned children.	Personal information provided will be used to create an account for students, so they are able to access the services offered by Microsoft Office365. Microsoft does not mine data for advertising purposes and all data remains the properly of the Kambrya College or the creator of the data
Who will be able to see the content and work?	Users will need to be registered users of the Kambrya College ICT Network. Access to technical materials will be required at times by these vendors. These vendors require strict permission before viewing any of the data. User permissions will be determined by the college ICT Manager and College Leadership team.	
Whilst students own copyright in the work they produce, who will have rights to reproduce and/or use the works?	All three services state in their respective privacy statements that the data remains the property of Kambrya College and the owner of the data. In the event that the college wish to reproduce the work of a student, the college will liaise with the student of the data to obtain their consent.	