

DIGITAL LEARNING POLICY

(INTERNET, SOCIAL MEDIA AND DIGITAL DEVICES)



Help for non-English speakers

If you need help to understand the information in this policy please contact the Principal, Stewart Milner.

CONTEXT

The Centre for Higher Education Studies (CHES) is a co-educational, specific purpose, senior secondary school where high-achieving and high-ability (HA) students can extend their learning. CHES offers face to face learning at a state-of-the-art facility in South Yarra and hosts a high-quality virtual platform to enable students to access programs at CHES regardless of where they are located.

Students engage with CHES programs in the following ways:

- direct enrolment of students into select VCE subjects onsite and virtually, including access to Student Enrichment Programs - providing mentoring, workshops, and seminars
- direct enrolment of Higher Education Studies (HES) delivered by partner Universities, including access to Student Enrichment Programs - providing mentoring, workshops, and seminars.

Students participating in CHES programs remain enrolled at their chosen secondary school (base school) and are supported to undertake a course at CHES as part of their VCE program. Working in close partnership with students' base schools, students will be enrolled in a CHES course for a fraction of their timetable (generally 20 per cent), with the remainder of their enrolment and timetable reflecting the subjects being completed at their base school.

CHES shares a joint responsibility with students' base schools to ensure students' social and emotional wellbeing, and also partners with Universities and base schools to ensure students' academic needs are met.

Individual student study arrangements are considered and agreed between the student, parent/carer, base school, and CHES upon enrolment and induction. To formalise individual student study arrangements CHES develop an Individualised Achievement Plan (IAP) which will include:

- study arrangements (CHES program and delivery mode - face to face, virtual, or combination)
- timetable requirements
- travel arrangements (if applicable)
- agreed communication methods between base-school and CHES (who, what, when and how)

- agreed communication methods between partner Universities and CHES (who, what, when and how)
- reasonable adjustments (if required)
- student health care needs including asthma management, administration of medication and individual anaphylaxis management
- cybersafety acceptable use agreement.

All CHES policies are designed to reflect its unique operating environment (physical and virtual), its program offerings, its partnerships with Universities and shared responsibility with students' base schools to ensure students' social and emotional wellbeing and academic needs are met.

CHES has a network of foundation schools and allows the member schools to deliver their own VCE classes within the CHES facility where not fully utilised for CHES programs. This policy does not consider CHES foundation school arrangements.

CHES has a Digital Learning policy to ensure that a safe and secure learning and teaching environment is provided for all students and staff.

PURPOSE

To ensure that all students and members of the CHES community understand:

- (a) our commitment to providing students with the opportunity to benefit from digital technologies to support and enhance learning and development at school, including engagement in and use of our Learning Management System and Virtual Environment
- (b) expected student behaviour when using digital technologies including the internet, social media, and digital devices (including computers, laptops, tablets)
- (c) the school's commitment to promoting safe, responsible and discerning use of digital technologies, and educating students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and digital technologies
- (d) our school's policies and procedures for responding to inappropriate student behaviour on digital technologies and the internet
- (e) the various Department policies on digital learning, including social media, that our school follows and implements

SCOPE

This policy applies to all students and staff at CHES, including university staff delivering programs for CHES students.

Staff use of technology is also governed by the following Department policies:

- [Acceptable Use Policy for ICT Resources](#)
- [Cybersafety and Responsible Use of Digital Technologies](#)
- [Digital Learning in Schools](#) and
- [Social Media Use to Support Student Learning](#).

Staff, volunteers and school councillors also need to adhere to codes of conduct relevant to their respective roles. These codes include:

- The CHES Child Safety Code of Conduct
- [The Victorian Teaching Profession Code of Conduct](#) (teaching staff)

- [Code of Conduct for Victorian Sector Employees](#) (staff)
- [Code of Conduct for Directors of Victorian Public Entities](#) (school councillors)

DEFINITIONS

For the purpose of this policy, “digital technologies” are defined as digital devices, tools, applications and systems that students and teachers use for learning and teaching; this includes Department-provided software and locally sourced devices, tools and systems.

POLICY

Vision for digital learning at our school

The Centre for Higher Education Studies’ (CHES) mission is to excite and develop the full intellectual, social and emotional potential of high-achieving and high-ability (HA) Victorian senior students by delivering a suite of programs to stretch, challenge and enhance learning, with access to leading expertise, practices and technology in a purpose-built facility. CHES is a bridge between school and university, city and regions, research and learning, reaching and achieving. Our school values are Reach, Connection and Understanding.

The effective use of digital technologies is central to our goal of empowering students to be forward-thinking. At CHES we seek to strengthen provision for high-ability and high-achieving (HA) senior students across Victoria and to that end the use of digital technologies and virtual environments is crucial to improving access to tertiary courses, making enrichment and extension opportunities available state-wide, including for students in rural and regional areas and in priority cohorts. In addition, to develop and enhance teachers’ abilities to meet the needs of HA students, a key component of the professional learning we provide to teachers across the state will be the effective use of digital technologies and virtual environments.

To enable equitable access to CHES programs for HA students, including a particular focus on those in rural and regional areas or from priority cohorts, we harness technology to support the delivery of programs in CHES, and via virtual platforms for students unable to physically attend. We deploy a Hy-Flex approach to program delivery at CHES—flexibility in student attendance onsite will be supported through the use of digital resources and the virtual platform, enabling innovative teaching and learning and student collaboration, irrespective of their location.

The use of digital technologies is a mandated component of the Victorian Curriculum. We recognise that safe and appropriate use of digital technologies, including the internet, apps, computers and tablets, can provide students with rich opportunities to support learning and development in a range of ways.

Through increased access to digital technologies, students can benefit from learning that is interactive, collaborative, differentiated, engaging and transformative. Digital technologies enable our students to interact with and create high quality content, resources and tools. It also enables personalised learning tailored to students’ particular needs and interests and transforms assessment, reporting and feedback, driving new forms of collaboration and communication.

CHES firmly believes that the use of digital technologies fosters the development of valuable skills and knowledge and prepares students to thrive in our globalised and inter-connected world. Our school’s vision is to empower students to use digital technologies safely and appropriately to reach their personal best and fully equip them to make significant contributions to society.

Personal Devices at CHES

Curriculum at CHES is delivered on-site and through a Learning Management System and Virtual Environment with the use of iPads/tablets/notebook computers. Students must bring a charged device—iPad, tablet, notebook computer—to school each lesson to be used during class time for different learning activities.

Our school operates a Bring Your Own Device (BYOD) program, which means students must bring their own purchased or leased device with them to school each day.

Specifications

Students will need to log in to the CHES Learning Management System (LMS) and Virtual Environment (VE) to engage in lessons and programs, access curriculum, communicate with teachers and submit work online regularly. They are expected to participate in various aspects of the online courses, including virtual classes, forums and interactive activities.

To have the best experience at CHES, students should have a device that is able to join live classes with a camera and a microphone. It can be beneficial to use a headset microphone for better audio quality, but in-built device microphones can also be used. It is also recommended that students have a device with a physical keyboard to easily take notes and respond to communication. Most desktops or laptops are compatible with our CHES LMS and VE.

Please note that a smartphone, tablet or Chromebook is insufficient to meet the needs of CHES programs. Where possible, it is recommended that more than one device is available if more than one child is enrolled at CHES in the same family.

Minimum Technical Specifications

It is recommended that students have a device that is able to:

- access the internet
- run Windows 10 or Mac OSX 10.13
- Have a core i5 processor (or greater)
- minimum 6 hours battery life
- minimum 4Gb RAM
- include HDMI or display port
- have a full size physical keyboard
- run a current web browser (e.g. Firefox, Safari or Chrome)
- run programs to create documents, spreadsheets and presentations
- enable the use of a web camera and headset
- install subject specific software where needed (please see individual subject information in CHES Handbook)
- be brought to school in a protective case.

Please note that CHES does not have insurance to cover accidental damage to students' devices, and parents/carers are encouraged to consider obtaining their own insurance for their child's device.

CHES liaises and works closely with the base schools of students to ensure that arrangements are in place to support families who may be experiencing long or short-term hardship to access devices.

Students, parents and carers who would like more information or assistance regarding our virtual learning environment are encouraged to contact the IT Manager or Principal. CHES uses a Learning Management System (Compass) to coordinate communications with students, parents/guardians, base schools and university partners. For support in using their laptop devices or for other hardware issues, students should refer to their base school in the first instance. If students are having difficulties logging into and accessing online classes as part of their CHES VCE studies or Higher Education Studies, the CHES IT manager is available through a designated contact email. CHES works closely with university staff to ensure that students are able to access online content.

Safe and appropriate use of digital technologies

Digital technologies, if not used appropriately, may present risks to users' safety or wellbeing. At CHES, we are committed to educating all students to use digital technologies in ways that respect the dignity of ourselves and others and promote full flourishing for all, equipping students with the skills and knowledge to navigate the digital world.

At CHES, we:

- use online sites and digital tools that support students' learning, and focus our use of digital technologies on being learning-centred
- use digital technologies for specific purpose with targeted educational or developmental aims
- supervise and support students using digital technologies (through both subject teachers, IT managers, and base school supervisors when students are learning remotely)
- effectively and responsively address any issues or incidents that have the potential to impact on the wellbeing of our students
- have induction programs in place to educate our students to be safe, responsible and discerning users of digital technologies
- educate our students about digital issues such as privacy, intellectual property and copyright, and the importance of maintaining their own privacy and security online
- actively educate and remind students of our Student Engagement Policy that outlines our CHES values and expected student behaviour, including online behaviours
- have an Acceptable Use Agreement outlining the expectations of students when using digital technologies for their learning at CHES
- use clear protocols and procedures to protect students working in online spaces, which includes reviewing the safety and appropriateness of online tools and communities and removing offensive content at the earliest opportunity
- educate our students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and other digital technologies
- provide a filtered internet service at school to block access to inappropriate content
- refer suspected illegal online acts to the relevant law enforcement authority for investigation
- support parents and carers to understand the safe and responsible use of digital technologies and the strategies that can be implemented at home through regular updates in our newsletter, information sheets, website/school portal and information sessions.

Student use of digital technologies at school will only be permitted where students and their parents/carers have completed a signed Cybersafety Acceptable Use Agreement.

It is the responsibility of all students to protect their own password and not divulge it to another person. If a student or staff member knows or suspects an account has been used by another person, the account holder must notify the IT manager or Principal, immediately.

All messages created, sent or retrieved on the school's network are the property of the school. The school reserves the right to access and monitor all messages and files on the computer system, as necessary and appropriate. Communications, including text and images may be required to be disclosed to law enforcement and other third parties without the consent of the sender.

Social media use

Our school follows the Department's policy on [Social Media Use to Support Learning](#) to ensure social media is used safely and appropriately in student learning and to ensure appropriate parent notification occurs or, where required, consent is sought. Where the student activity is visible to the public, it requires consent. At CHES we use the DET social media consent form template available at [Social Media Use to Support Learning](#).

CHES uses Facebook and Instagram to showcase student learning. Parents are welcome to contact the Principal if they have any questions or concerns about students participating in this school social media. CHES also publishes a newsletter and other content on our public website. The school only uses the images of students on this platform after they have signed a specific permission form.

CHES also synchronises photographs of students to Compass and the Office 365 suite to enable clear identification of students when marking the roll and communicating within closed online classroom spaces.

In accordance with the Department's policy on social media, CHES staff and university staff who are involved in CHES programs will not 'friend' or 'follow' a student on a personal social media account, or accept a 'friend' request from a student using a personal social media account unless it is objectively appropriate, for example where the student is also a family member of the staff. The social media policy expectations are included in the University Partnership Agreements in terms of child safety requirements and obligations.

If a staff member of our school becomes aware that a student at the school is 'following' them on a personal social media account, Department policy requires the staff member to ask the student to 'unfollow' them, and to notify the school and/or parent or carer if the student does not do so.

Student behavioural expectations

When using digital technologies, students are expected to behave in a way that is consistent with the CHES *Statement of Values, Student Wellbeing and Engagement Policy, and Bullying Prevention Policy*.

When a student acts in breach of the behaviour standards of our school community (including cyberbullying, using digital technologies to harass, threaten or intimidate, or viewing/posting/sharing of inappropriate or unlawful content), CHES will institute a staged response, consistent with our student engagement and behaviour policies.

Breaches of this policy by students can result in a number of consequences which will depend on the severity of the breach and the context of the situation. This includes:

- removal of network access privileges
- removal of email privileges
- removal of internet access privileges
- removal of printing privileges
- other consequences as outlined in the school's *Student Wellbeing and Engagement and Bullying Prevention* policies.

Supervision of student in emergency operating environments

In the event of any mandatory period of remote or flexible learning our School will follow the operations guidance issued by the Department.

COMMUNICATION

This policy will be communicated to our school community in the following ways:

- available publicly on our school's website
- included in staff induction processes, including induction for university staff who are delivering programs through CHES
- discussed at staff briefings/meetings as required
- included in our staff handbook and our base school supervisor handbook
- discussed at parent information nights/sessions
- included in transition and enrolment packs
- discussed at student forums/through communication tools
- made available in hard copy from school administration upon request.

POLICY REVIEW AND APPROVAL

Policy last reviewed	February 2022
Consultation	Consultation with staff, students and school council to take place in 2023 after operations commence
Approved by	Principal, Stewart Milner
Next scheduled review date	February 2023 - to ensure ongoing relevance and continuous improvement, this policy will be reviewed every 1-2 years thereafter.

* The Digital Learning Policy will be reviewed and approved by the School Council once they are appointed.

SAFE CONNECTIONS

CYBER SAFETY &

ACCEPTABLE USE AGREEMENT FOR STUDENTS

Section A:	Introduction
Section B:	Cyber Safety Code of Conduct for Students
Section C:	Student Cyber Safety Use Agreement Form

Instructions:

1. Students and parents*/caregivers/legal guardians please read and discuss all sections carefully.
2. Parents and students sign section C.
3. If you have any questions about this agreement, please contact the school.

* The term 'parent' used throughout this document also refers to legal guardians and caregivers.

Important terms used in this document:

1. The abbreviation 'ICT' in this document refers to the term 'Information and Communication Technologies';
2. 'Cybersafety' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones;
3. 'School ICT' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below;
4. The term 'ICT equipment/devices' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use;
5. 'Objectionable' in this agreement means material that deals with matters such as sex, cruelty, or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school environment. This is intended to be inclusive of the definition used in the Films, Videos and Publications Classification Act 1993;
6. 'DET' Department of Education and Training

SECTION A

Introduction:

The measures to ensure the cyber safety of students at the Centre for Higher Education Studies (CHES) outlined in this document are based on our core values. The school's computer network, Internet access facilities, computers and other school ICT equipment/ devices bring great benefits to the teaching and learning programs at CHES, and to the effective operation of the school. Our school has rigorous cyber safety practices in place, which include cyber safety use agreements for all school staff and students.

The overall goal of the school in this matter is to create and maintain a cyber safety culture which is in keeping with the values of the school, and legislative and professional obligations. This use agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cyber safety breaches which undermine the safety of the school environment.

All students will be issued with a use agreement and once signed consent has been returned to school, students will be able to use the school ICT equipment/devices.

The school's computer network, Internet access facilities, computers and other school ICT equipment/devices are for educational purposes appropriate to the school environment. This applies whether the ICT equipment is owned or leased either partially or wholly by the school, and used on or off the school site.

SECTION B

Code of Practice to Help Keep CHES Students Cyber Safe:

1. As a safe and responsible user of ICT I will help keep myself and other people safe by following this Code of Practice
2. I cannot use school ICT equipment until my parent and I have read and signed my use agreement form (see Section C) and returned it to CHES.
3. If I have my own username, I will log on only with that username. I will not allow anyone else to use my username
4. I will not tell anyone else my password.
5. While at school or a school-related activity, I will not have any involvement with any ICT material or activity which might put myself or anyone else at risk (e.g. bullying or harassing).
6. I understand that I must not at any time use ICT to upset, offend, harass, threaten or in any way harm anyone connected to the school or the school itself, even if it is meant as a joke.
7. I understand that the Code of Practice in this use agreement also apply to mobile phones. I will only use my mobile phone(s) at the times that I am permitted to during the school day.
8. I understand that I can only use the Internet at school when a teacher gives permission and there is staff supervision.
9. While at school I will not:
 1. Access, or attempt to access, inappropriate, age restricted, or objectionable material;
 2. Download, save or distribute such material by copying, storing, printing or showing it to other people; and
 3. Make any attempt to get around or bypass security, monitoring and filtering that is in place at school.
10. If I accidentally access inappropriate material, I will:
 - Not show others;
 - Turn off the screen or minimise the window; and
 - Report the incident to a teacher immediately.
11. I understand that I must not download any files such as music, videos, games or programs without the permission of a teacher. This makes sure the school complies with the Copyright Act 1968. I also understand that anyone who infringes copyright may be personally liable under this law.
12. I understand that this Code of Practice applies to any privately owned ICT equipment/device (such as a laptop, mobile phone, USB drive) I bring to school or a school-related activity. Any images or material on such equipment/ devices must be appropriate to the school environment.

13. I will not connect any device (such as a USB drive, camera or phone) to, or attempt to run any software on, school ICT without a teacher's permission. This includes all wireless technologies.
14. I will ask a teacher's permission before giving out any personal information (including photos) online about myself or any other person. I will also get permission from any other person involved. Personal information includes name, address, email address, phone numbers, and photos.
15. I will respect all ICT systems in use at school and treat all ICT equipment/devices with care. This includes:
 1. Not intentionally disrupting the smooth running of any school ICT systems
 2. Not attempting to hack or gain unauthorised access to any system
 3. Following the school's cyber safety Code of Practice, and not joining in if other students choose to be irresponsible with ICT; and
 4. Reporting any breakages/damage to a staff member.
16. I understand that the school may monitor traffic and material sent and received using the school's ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including email.
17. I understand that the school may audit its computer network, internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit. Auditing of the above items may include any stored content, and all aspects of their use, including email.
18. I understand that if I contravene the Code of Practice, the school may inform my parent(s). In serious cases the school may take disciplinary action against me. I also understand that my family will be charged for repair costs. If illegal material or activities are involved, it may be necessary for the school to inform the police.

SECTION C

CYBER SAFETY USE AGREEMENT:

To the student and parent/legal guardian/caregiver, please:

1. Read this page carefully to check that you understand your responsibilities under this agreement;
2. Sign the appropriate section on this form; and
3. A copy of this document is in the Policies Book for your future reference.

We understand that CHES will:

1. Do its best to keep the school cyber safe, by maintaining an effective cyber safety program. This includes working to restrict access to inappropriate, harmful or illegal material on the Internet or school ICT equipment/ devices at school or at school-related activities, and enforcing the cyber safety Code of Practice and requirements detailed in use agreements;
2. Keep a copy of this signed use agreement form on file;
3. Respond appropriately to any breaches of the user agreements;
4. Provide members of the school community with cyber safety education designed to complement and support the use agreement initiative; and
5. Welcome enquiries from students or parents about cyber safety issues.

SECTION FOR STUDENT:

My responsibilities include:

1. I will read this cyber safety use agreement carefully;
2. I will adhere to this acceptable use agreement and cyber safety Code of Practice and instructions whenever I use the school's ICT;
3. I will also follow the cyber safety Code of Practice whenever I use privately-owned ICT on the school site or at any school-related activity, regardless of its location;
4. I will avoid any involvement with material or activities which could put at risk my own safety, or the privacy, safety or security of the school or other members of the school community;
5. I will take proper care of school ICT. I know that if I have been involved in the damage, loss or theft of ICT equipment/devices, my family will have responsibility for the cost of repairs or replacement; and
6. I will ask my CHES teacher or CHES principal, if I am not sure about something to do with this agreement.
7. I will bring my devices fully charged to CHES lessons.
8. I will back up data securely, including my VCE school-assessed coursework as per VCAA requirements.
9. I will carry my device in an appropriate protective case at all times.
10. I will take care of my device and will not leave it unattended in bags, classrooms or public spaces around CHES.

When I use digital technologies, the Learning Management System and 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 writing or participating in online bullying (e.g. forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviours)
- protecting my privacy; not giving out personal details, including my full name, telephone number, address, passwords and images
- protecting the privacy of others; never posting or forwarding their personal details or images without their consent
- contacting a teacher or a trusted adult if I personally feel uncomfortable or unsafe online

- contacting a teacher or a trusted adult if I see others participating in unsafe, inappropriate or hurtful online behaviours
- contacting a teacher or a trusted adult if someone writes something I don't like, makes me and/or my friends feel uncomfortable or requests information from me I know is private
- carefully considering the content that I upload or post online; knowing that this is a personal reflection of who I am and what people may think of me
- investigating the terms and conditions of use of the websites I sign up to as part of the learning program (e.g. age restrictions, parental consent requirements) and if my understanding is unclear seeking further explanation from a trusted adult
- confirming that I meet the stated terms and conditions and completing the required registration processes
- abiding by copyright and intellectual property regulations; requesting permission to use images, text, audio and video and cite references where necessary
- not downloading unauthorised programs, including games while using the school's ICT equipment
- not interfering with network systems and security, the data of another user or attempting to log into the network with a user name or password of another student, parent/carer, school staff member
- not reveal my password to anyone including teachers or administrators at the school
- use social networking sites for education purposes and directed by the school
- not deliberately enter or remain in any site that has obscene language or offensive content

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

- respecting the privacy of others; only taking photos or recording sound or video when others are aware and formal consent has been provided as part of an approved learning program
- respecting others and communicating with them in a supportive manner, including outside school hours and in social contexts by not making harassing phone calls/text messages or forwarding on messages
- obtaining appropriate (written) consent from individuals who appear in images or sound and video recordings before forwarding them to other people or posting/uploading them to online spaces.

I have read and understood my responsibilities and agree to abide by this cyber safety use agreement. I know that if I breach this use agreement there may be serious consequences, which may result in expulsion.

Name of student:

Signature:

Date:

SECTION FOR PARENT/LEGAL GUARDIAN/CAREGIVER:

My responsibilities include:

11. I will read this cyber safety use agreement carefully and discuss it with my child so we both have a clear understanding of their role in the school's work to maintain a cyber safe environment;
12. I will ensure this use agreement is signed by my child and by me, and returned to the school;
13. I will encourage my child to follow the cyber safety rules and instructions; and
14. I will contact the school if there is any aspect of this use agreement I would like to discuss.
15. Damage or loss of equipment—as a parent I am responsible for making sure the device is covered under my insurance, so that it can be replaced if lost or damaged and I will notify CHES if the device is damaged or lost so that my child's learning program is not interrupted whilst being replaced.
16. I will ensure that the device has appropriate virus protection

I have read this Cybersafety Use Agreement document and am aware of the school's initiatives to maintain a cyber safe learning environment, including my child's responsibilities.

Name of Parent/Guardian:.....

Signature:

Date:

Please note: This agreement for your child will remain in force as long as they are enrolled in a CHES program. If it becomes necessary to add/amend any information or the Code of Practice, parents will be advised in writing.