

HAWKESDALE P12 COLLEGE



Electronic Device & Internet Usage Policy

Hawkesdale P12 College believes the teaching of cybersafe and responsible online behaviour is essential in the lives of students and is best taught in partnership between home and school.

21st century students spend increasing amounts of time online, learning and collaborating. To be safe online and to gain the greatest benefit from the opportunities provided through an online environment, students need to do the right thing by themselves and others online, particularly when no one is watching.

Safe and responsible behaviour is explicitly taught at our school and parents/carers are requested to reinforce this behaviour at home.

Some online activities are illegal and as such will be reported to police.

Our school will be an eSmart school and promote cybersafety in the community.

The link to the DET consent, acceptable use agreements and online services is <http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/loiconsent.aspx>

Part A - School support for the safe and responsible use of digital technologies

Hawkesdale P12 College uses the internet and digital technologies as teaching and learning tools. We see the internet and digital technologies as valuable resources, but acknowledge they must be used responsibly. Your child has been asked to agree to use the internet and mobile technologies responsibly at school. Parents/carers should be aware that the nature of the internet is such that full protection from inappropriate content can never be guaranteed.

At Hawkesdale P12 College we:

- Have a **Student Engagement and Wellbeing 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
- Have programs in place to educate our students to be safe and responsible users of digital technologies such as cyber safety sessions, adolescent health classes and use of online blogs
- Provide information about digital access issues such as online privacy, intellectual property and copyright
- Supervise and support students using digital technologies in the classroom
- 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 – please refer to the following site for additional information about duty of care
 - Duty of Care and Supervision
(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
(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>)

Part B - Student Agreement

By signing the Acceptable Use Agreement, students agree to the following:

- 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 individual privacy by not giving out personal details, including 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 they personally feel uncomfortable or unsafe online, or if they see others participating in unsafe, inappropriate or hurtful online behaviour
- Thinking carefully about the content uploaded or posted online, knowing that this is a personal reflection of identity and can influence perceptions of the posting student
- Review the terms and conditions of use for any digital or online tool (e.g. age restrictions, parental consent requirements), and if understanding is unclear seek 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
- Allow the principal or his representative to examine my electronic device if there is a reason to believe inappropriate material is on it

Mobile Phones:

- Follow the school mobile phone policy by handing in their phone during form assembly and collect it at the end of the day or by not bringing to school at all. Students are not permitted to have phones with them during the school day.

Using a digital device as a camera:

- Only take photos and record sound or video when it is part of a class or lesson.
- Seek permission from individuals involved before taking photos, recording sound or videoing them (including teachers).
- Seek appropriate (written) permission from individuals involved before publishing or sending photos, recorded sound or video to anyone else or to any online space.
- Be respectful when taking photos or video and never use these as a tool for bullying.

INTERNET USAGE

RATIONALE

- Respectful and effective use of the internet provides students with unprecedented opportunities to obtain information, engage in discussion, and liaise with individuals, organisation and groups world-wide so as to increase skills, knowledge and abilities.

AIMS

- To improve student learning outcomes by increasing access to world-wide information.
- To develop skills in discriminate and appropriate internet and computer usage.

IMPLEMENTATION

- Our school actively supports access by students to the widest variety of information resources available, accompanied by the development of the skills necessary to filter, analyse, interpret and evaluate information encountered.
- All students and staff at our school will have censorship filtered internet and email access. All students and staff will have their own password protected internet account and log on. Such access is a privilege that infers responsibility, and not simply a right to be expected.
- Students will be held responsible for all activity that occurs under their log-in and password.
- Student behaviour when using school computers and networks, when using the internet and e-mail, and when engaging in any activity with school computers must be consistent with the school's Acceptable User Agreement.
- Technical support is provide, in conjunction with the principal, to manage all e-mail access, maintenance of the school's web site, web filters, and all other issues related to internet access by students and teachers.
- The school undertakes to ensure that information published on the Internet by students or the school is of a high standard, and meets legal requirements and standards of general practice within the community in relation to copyright, safety and decency.
- Consequences of publishing, accessing or failing to notify the coordinator of inappropriate material shall include the removal of access rights.
- Upper Primary and Secondary – Years 5 to 12 - A signed parent and student Acceptable User Agreement is required to be completed in order to gain access to the internet, or to publish work, photos or videos on the internet.
- Privacy of students, parents, staff and other users must be recognised and respected at all times. Student's will only identify themselves on the internet by their first name and last initial.
- Staff are expected to utilise and integrate technologies, including on-line learning opportunities, into their programs for all students.
- The school will provide appropriate professional development and support for all staff.

Family Information – Advice to support the safe and responsible use of digital technologies at home

At school the internet is mostly used to support teaching and learning. At home, however, it is often used differently. Not only is it a study resource for students, but it is increasingly being used as a social space to meet and chat.

The term “space” is used here to describe a website that works like a community with live interaction and the capacity for your child to chat with others, personalise their space and share information. Each space has a purpose, audience and tool set including those around security and protection. The internet also provides access to websites with information, images videos for students to view. Not all content is presented as a space.

About the agreement:

In signing the Acceptable Use Agreement your child will be agreeing to behave in a certain way online and to take appropriate action when and as required. Elements of agreement are explained below. Please contact the school to clarify or receive additional information.

Be a safe, responsible and ethical user of online information, whenever and wherever it is accessed:

The school’s Student Engagement and Wellbeing Policy outlines the values of the school and expected behaviours when students use the internet and digital technologies at school.

Mutually respectful online behaviour:

Being online can make students feel that they are anonymous and sometimes students may say things online that they would never say to someone’s face. The web space or online chat environment that they use in leisure time might also have explicit language and they may feel they have to be part of it. Bullying online can take a number of forms from repeated messages to exclusion from social spaces. Students who forward on messages or participate in the exclusion may not see themselves as bullying. These actions also contribute to the hurt and distress of others.

Talk to a teacher or trusted adult if students feel uncomfortable or unsafe online or see others participating in unsafe, inappropriate or hurtful online behaviour:

Incidents online often go unreported. Students have reported their reasons as embarrassment, a belief that online issues are theirs to solve as adults don’t understand, a feeling that reporting it will make it worse and the most common reason given is a fear that they will lose access to their technology.

Students are advised to report an incident if:

- they feel that the welfare of other students at the school is being threatened
- they come across sites which are not suitable for their school
- someone writes something they don’t like, or makes them and their friends feel uncomfortable or asks them to provide information that they know is private
- they accidentally do something which is against the rules and responsibilities they have agreed to.

Seek to understand the terms and conditions of websites and online communities and be aware that uploaded and posted content constitutes an individual’s digital footprint:

Many websites/spaces have conditions of use, such as ownership of the content and the age of participants. For example: Children under 13 years of age are not permitted access to Facebook. When posting information online - A good rule is “Don’t post what you wouldn’t want your Grandparent, Principal, or future boss to read.”

Protect my privacy rights and those of other students by not giving out personal details including full names, telephone numbers, addresses and images.

Students like to publish information about themselves and their friends in spaces like Facebook and blogs. This can put them at risk of being approached, groomed or bullied online. To avoid this we recommend they:

- don't use their own name, but develop an online name and use avatars
- don't share personal details, including images of themselves or their friends online
- password protect any spaces or accounts they have
- don't allow anyone they don't know to join their chat or collaborative space
- are reminded that any image or comment they put on the internet is now public (anyone can see, change or use it) so no full names should appear in reference to individuals in any image, movie or sound recording
- ALWAYS make the space private so that they can control who sees their space and can communicate with them
- understand the terms and conditions of any website or online community that they might join.

Use the internet at school for educational purposes and use the equipment properly

It is important to realise that there is a time for fun and a time for work on the internet. Students may often see the internet as 'free' however even just looking at a page on the internet incurs a download cost. By taking care with the equipment, and thinking carefully about printing and downloading from the internet students can save time, money and the environment. Staying on task will reduce the risk of inappropriate access and teach students strategies to use the internet or mobile technologies for their learning.

Use social networking sites for educational purposes and only as directed by teachers

Web 2.0 tools and social networking spaces allow students to be contributors to the web and to work collaboratively online with other students. Creating or contributing to blogs, wikis, digital stories and podcasts can all be legitimate educational activities which allow students to publish, share and inform others and be active contributors to the web. It is important for students to understand that working in a collaborative space as part of a learning task, has a very different purpose to using a social networking space to link up with friends in their own time.

Abide by copyright procedures when using content on websites (ask permission to use images, text, audio and video and cite references where necessary)

Music, information, images and games on the internet are owned by someone. The term copyright is a legal one and there are laws to enforce it. Not only is breaking copyright morally, ethically and legally wrong, it can introduce potential risks. By downloading a 'freebie' you can risk bringing a virus or spyware to the computer or system. These can destroy a computer system or provide hackers with details such as passwords and bank accounts. Peer to peer sharing software like Limewire and Bit-torrent can sometimes share music and files illegally, and make computers vulnerable.

Think critically about other users' intellectual property and how content sourced from websites can be used in student work

Not everything on the internet is true, accurate or unbiased. The school is working to teach digital literacy skills, which enable students to locate, evaluate, and use information effectively on the internet. It is important that your child respects the Intellectual Property of people who contribute resources online. Students should use their own thoughts and language to express what they have learnt, and avoid simply copying and pasting information from the internet.

Not interfere with network security, the data of another user or attempt to log into the network with a user name or password of another student

- Not reveal personal passwords to anyone except the system administrator or classroom teachers
- Not bring or download programs without permission, including games, to the school or run them on school computers
- Not deliberately enter or remain in any site that has obscene language or offensive content (e.g. racist material or violent images)

In school settings internet service providers set up filters to block out a lot of inappropriate content, but these filters are not always foolproof. Students, who deliberately seek out inappropriate content or use technologies which bypass filters, will have their internet access reviewed and their parent/carers will be immediately informed.

Computer facilities are for the use of all students so due care should be taken at all times when using these resources. Students are responsible for everything done using their accounts, and everything in their home directories. To this end, students need to keep their password secret and not gain access to other students' login details. The school connects all of the computers through a network. The introduction of unknown games or files could introduce viruses, etc and these put all school equipment and student work at risk.

When using a digital device as a camera students will:

- Only take photos and record sound or video when it is part of a class or lesson.
- Seek permission from individuals involved before taking photos, recording sound or videoing them (including teachers).
- Seek appropriate (written) permission from individuals involved before publishing or sending photos, recorded sound or video to anyone else or to any online space.
- Be respectful in the photos I take or video I capture and never use these as a tool for bullying.
- Any photo or recording must be deleted off the device once it is no longer required.

The recording of images and sounds can breach students' rights under the Privacy Act. Sometimes students are reluctant to tell their peers that they don't want their image or voice recorded. The Privacy Act says that the posting and sharing of information online or in any other way requires consent.

This consent must be **fully informed, freely given, current** and **specific** in how the information will be presented and who it will be presented to. Schools are required to obtain signed authority for any work, images or information posted online. All citizens need to respect the rights of others to privacy and students are no exception. A sample consent form for requesting permission is available on the DET website. Consent can be withdrawn at anytime.

<http://www.education.vic.gov.au/management/elearningsupportservices/www/formstemp.htm#H2N10064>

Bridging the gap between home and school

At school the internet is mostly used to support teaching and learning. At home, however, it is often used differently. Not only is it a study resource for students, but it is increasingly being used as a social space to meet and chat.

If you have the internet at home, encourage your child to show you what they are doing online.

At home we recommend you:

- find out how your child uses the internet and who else is involved in any online activities
- have the computer with internet access in a shared place in the house – not your child's bedroom
- ask questions when your child shows you what they are doing, such as:
- how does it work and how do you set it up?

- who is else is sharing this space or game? (do you know them or did you 'meet' them online?)
- can you see any risks or dangers in the activity - what would you say to warn/inform a younger child?
- what are you doing to protect yourself or your friends from these potential dangers?
- when would you inform an adult about an incident that has happened online that concerns you? (Discuss why your child might keep it to themselves.)

Statistics show that students will not approach an adult for help because:

- *they might get the blame for any incident*
- *they don't think adults "get" their online stuff*
- *they might put at risk their own access to technology by either:*
- *admitting to a mistake or*
- *highlighting a situation that might lead a parent to ban their access.*

Scenarios for teacher/parent/guardian/student discussion:

What do you do?

- You found the car picture you were searching for, but it includes a naked woman!
- Someone keeps messaging nasty and upsetting comments about you and your friends on your mobile phone.
- A person you met online asks you to give them your full name, phone number and suggests you meet. Is it different if they have been your "friend" for a long time?
- You are sent a message which has been forwarded by someone else. It has embarrassing comments/image about someone you know.
- A game online will only let you play it if you give your name, address, date of birth, etc.
- An online community asks you to sign up and allow the space to "Connect you to all your friends" It wants your email address and password to do this. It needs access to your address book.
- In an online space/chat someone suggests you all exclude /block a classmate.
- Your friend took a video of you and your friends 'mucking around' and posted it on a video hosting service like YouTube.
- You told your parent/guardian that you are doing homework for hours every night on the computer.
- Your friend has an online profile published (not set to private). You can see their personal details and photos. Other people you know are in the photos.
- A friend tells you about a great site where there is 'free' music or a game to download.

Key Discussion Questions for parents to ask

At home we recommend you make some time to find out how your child is using the internet. Make some time to sit with them online and ask questions such as:

- What is it that is so enjoyable about the site or space you are using? What is the purpose of the site or space?
- How does it work? How do you set it up? What are the conditions of use?
- Who is else is sharing this space? Do you know them or did you 'meet' them online? How can you control who is in your space?
- Can you see any risks or dangers in the activity? What would you say to warn/inform a younger child?
- What are you doing to protect yourself or your friends from these potential dangers?
- When would you tell an adult about an incident that has happened online? Who would you tell?
- When wouldn't you tell and why not? Research shows that students are reluctant to report issues and put at risk their internet/phone access.

Encourage your child to set their space to 'private' if they use a social networking site like Myspace, Bebo or Facebook (they are then in control of who can contact them and access their information).

Ensure that all internet activities occur in a shared place– not your child's bedroom. Negotiate appropriate times for online activities and use of mobile phones. Consider the use of "safe search filters" freely available as settings on Google, Bing etc.

Reference:

- This policy has been developed in conjunction with the DET's School Policy and Reference Guide <http://www.education.vic.gov.au/school/principals/spag/Pages/spag.aspx>.

Evaluation:

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

School Council President

Principal

This policy was ratified by school council on