Heathfield High School
Information Technology
Cyber Safety & Acceptable Use Policy
Version 0915

This policy applies whenever you are using Heathfield High School Information Technology equipment or services. It should be read in conjunction with the Heathfield High School Laptop Use Policy. In some cases, conditions of the Heathfield High School Laptop Use Policy will override or modify conditions in this policy. Where this is the case, students must ensure that they apply those conditions only when using their personal laptop computer. When using school workstations, the conditions stated in this policy will apply.

Heathfield High School is committed to providing a cyber-safe learning environment. Your use of Heathfield High School's Information Technology resources, including school-located computers, student laptops (whether used at school or at home), or internet access must be in accordance with the information contained in this policy at all times.

Cyber Safety

You have a responsibility to ensure the safety of yourself and others when accessing IT resources. IT resources include computers (such as desktops, laptops and tablets), storage devices (such as USB and flash memory devices, CDs, DVDs, iPods, MP3 players), cameras (such as video and digital cameras and web-cams), all types of mobile phones, gaming consoles, video and audio players or receivers (such as portable CD and DVD players), and any other similar technologies

- You should only access or attempt to access, download, save and/or distribute age-appropriate and relevant material.
- You must not access inappropriate material. This includes material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children, or incompatible with a school environment.
- You must ensure that any privately-owned IT resources that you bring to school do not contain any inappropriate material.
- If you accidentally access inappropriate material, immediately minimise the screen window, or turn off the monitor, and inform a teacher immediately. You must not show others.
- You should only use the internet, email, or IT resources for positive purposes; not to be mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the school itself, even if it is meant as a joke.
- You must report any activity using IT resources, including bullying or harassing, which might make you or any other person feel uncomfortable, or put you or any other person at risk.
- To ensure that your privacy and safety are maintained, you should not put any personal information on publicly-accessible websites or social networking sites. This includes your full name, address, phone numbers, email address, financial details such as credit card numbers, or photos and/or videos of yourself or close friends.
- To ensure your compliance with copyright laws, you should only download or copy files such as music, videos, games or programs with the permission of a teacher or the owner of the original material.

Cyber Bullying

Cyber bullying is bullying which uses electronic technology as a means of victimising others. It includes the use of an internet service or mobile technologies, such as email, chat rooms, discussion groups, instant messaging, webpages or SMS text messaging, with the intention of harming another person.

- Examples of cyber bullying can include communications that seek to intimidate, control, manipulate, put down, or humiliate the recipient. Activities can include flaming (repeated negative messages), sexual and racist harassment, denigration, impersonation, trickery, exclusion and cyber stalking.
- The recording of a person's voice or image without permission is illegal and the uploading of such files to the internet can constitute cyber bullying.
- Cyber bullying may involve varying levels of severity, ranging from occasional messages to frequently-repeated and highly-disturbing threats to a person's life. Cyber bullying can therefore constitute an electronic crime.

Electronic Crime (E-Crime)

Electronic crime occurs when computers, or any other electronic communication equipment or devices (such as mobile phones or the internet), are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

- Where a student is suspected of an electronic crime, the matter will be reported to the South Australian Police.
- When it is suspected that a personal electronic device such as a mobile phone is used to capture images of a crime (such as an assault), or contains any other evidence of a crime, the device will be confiscated and handed to the police.
- These actions may be taken even if the alleged incident occurs off-site and/or out of school hours.

User-Names and Passwords

Access to the network is only allowed through your individual network account, which has a unique username and password.

- You will be responsible for any and all use of the network, including the cost of printing, Internet access, email access and disk storage, or actions such as harassment, bullying or accessing inappropriate material, which occurs using your username and password.
- You must keep your password secret. You must memorise your password, and not write it down anywhere. If you write your password down, or leave your password slip lying around, and someone else learns your password, they will be able to use your printing and internet accounts, and you will be responsible for the cost and their actions.
- You must not share your username and password with anyone, other than your parent(s) or caregiver(s).
- If you suspect that someone has learnt your password, report the matter immediately to one of the IT staff.
- When you finish using a computer, you must log-off using the “Log off …” option on the Start menu. If you do not, another user will be able to print or access the Internet using your username and password, and you will be responsible for the cost and their actions.
- You must only log-on to the network using your own username and password. If you access the network using another user’s username and password, or deliberately allow another student to access the network using your username and password, both accounts will immediately be disabled. In addition, other consequences will follow.
- If you forget your password, you will need to contact one of the IT staff to have a new one issued to you. An administration fee of $5.00 may be charged for a password reset.

Storing Data Files

To make sure that your data is safe and backed-up, it is very important that you only save files on the network servers.

- You have been given your own folder on the network in which you must save your personal files. This folder appears as your “Documents” folder. Everything that you save should be saved in “Documents”. You must not save files in any other location on the network, or on the hard disk of a school workstation you are using, unless a staff member has given you specific permission to do so.
- You must not save documents to your desktop, as this increases the time it will take for you to log-on or log-off the network.
- If you need to work on files at home, you should save those files on a USB memory device, or email them to your home email account.
- You are responsible for all information saved in your personal folder, as nobody can access your personal folder unless they know your username and password.
- You should be aware that your personal folders will be monitored by IT staff and/or teaching staff to ensure that you are not saving inappropriate material.

Care of the Network

You have a responsibility to treat the school’s computing resources (hardware, software, network, furniture, etc.) with respect.

- You must not take your bag(s) into any of the computing rooms. All bags must be placed on the racks provided outside the computing rooms. As this is a safety issue, all bags not placed in bag racks may be removed from the area, and may only be collected at a time convenient to the school.
- You must not eat or drink in any of the computing rooms, or while using any of the school’s computers.
- You must leave the computing area neat and tidy when you have finished working.
- You must report any problems with network equipment to a member of the IT staff.
- You must not attempt to connect, disconnect, move or otherwise interfere with any computers, monitors, mice, keyboards, printers, cables, or any other hardware.
- You must not connect any personal IT equipment such as laptop computers or mobile phones to the network, including by wireless, infrared or Bluetooth connections, unless you have been given specific permission to do so by a member of the IT staff.
- You must not attempt to access, create, delete or otherwise change any software or hardware settings, or interfere with the normal operation of the network in any way.
- School computers carry labels with identification numbers and/or barcodes, and operating system licence numbers. These labels must not be removed or damaged in any way. The removal of, or damage to, the operating system licence sticker invalidates the licence. If this occurs, you will be charged for the cost of an equivalent operating system licence.
- If you are responsible for any damage to a computer or other hardware, your IT account will immediately be disabled, and you will be charged for the cost of that damage. If the damage is wilful, police may be involved.
- Before you logon to any computer, you must check the computer for any existing damage. If you find any damage, it is your responsibility to report that damage to a member of the IT support staff immediately you logon to the computer. To do this, you should click on the ‘Report Computer Damage’ application on the Start menu. This application will automatically identify the computer and your user name. You should type a brief description of the damage, and then click on the ‘Submit’ button. Once you have done this, you can close the application and continue with your work. A member of the IT support staff will rectify the damage you have reported as soon as possible, and if necessary, steps will be taken to identify the student responsible for the damage.
- If you logon to a computer which is damaged, and you do not report the damage immediately, you may be held responsible for that damage.

Acceptable Use of the Network

The Heathfield High School computer system is provided for use related to your school studies only. You must follow the following guidelines.

- You must not use the computers for playing games at any time, including before or after school, or at recess and lunch times.
- You must not create, access, save, or send any material that contains common swear words, or that is violent, racist, sexist, pornographic, malicious, harassing, bullying, offensive, or illegal in any way.
- You must not download, save, access or run any games, utility programs or other executable programs (.exe, .com, .bat, .scr, .pif, etc.), either on the network file-servers, or on removable media such as USB devices used on the school network, other than those applications provided by the school.
- You must not attempt to spread any form of unsolicited email (spam) or chain letters, or any malicious software (such as viruses or worms).
- You must not use any kind of messaging program to send messages to other users of the network.
- You must respect the laws relating to copyright and intellectual property rights when using the network. You must not copy information from other students, the internet or any other source, unless the owner of that information has given permission for the material to be copied.
- You must not copy information and present that information as your own work. You must acknowledge the source of any information that you copy and include in your work.
- You should be aware that your use of the IT system is recorded in network logs, and is monitored by IT staff and/or teaching staff to ensure that you comply with this policy. If necessary, the school may commission an independent forensic audit that may cover any stored content, and all aspects of network use including email and internet access.

Printing

Printing is costly, and it is important to make sure that resources are not wasted by indiscriminate use of printers.

- You will be given a printing account with an initial credit at the start of each year.
- Your printing account will be charged for each page you print on any of the school's printers. The cost per page will depend on the size of the page, and whether it is black and white or colour.
- Information about your initial printing credit and the cost per page is subject to change. Current information is available on the school website at www.hhs.sa.edu.au. Click on About HHS | Policies | Information Technology.
- You can check the balance of your printing account at any time by clicking on the Start menu, and then selecting "Printing Account Status".
- When your printing account balance gets low, you can purchase additional printing credit from the cashier. This credit can be purchased in multiples of $1.00 or $5.00.
- If you need to print as part of your studies, it is your responsibility to ensure that you have adequate credit in your printing account to cover your printing needs.

Internet Access and E-mail

Heathfield High School provides access to the internet and an e-mail account to all students for educational use only. Heathfield High School policy is to maximise the use of the internet for educational purposes by providing internet access for educational use at no charge to students and parents. However, if a student abuses this policy and downloads large quantities of non-educational material (including, but not limited to, music, videos, movies, games, applications, torrents), the school retains the right to recoup the cost of those non-educational downloads from students and/or parents.

- You must only connect to the internet in the approved manner, using the school's proxy server. You must not attempt to bypass this server, connect to the internet using alternative internet access devices, connect to the internet using any anonymous proxy server, or bypass any security, filtering or monitoring in any way.
- You will be given an internet account with an initial download credit at the start of each year.
- Your internet credit will be charged each time you access the internet. This includes viewing web pages, sending or receiving emails, or downloading files.
- If an IT staff member determines that your use of the internet has been for non-educational use, additional credit will not be granted, and you will be liable for the cost of that non-educational use, and subject to the consequences of breaching this policy.
- You must not use the internet to access or send content such as emails, that contain common swear words, or that is violent, racist, sexist, pornographic, malicious, harassing, bullying, offensive, or illegal in any way.
- You must not download streaming audio or video from the internet unless you have been given specific permission to do so by a staff member or a member of the IT staff.
- You must not access any file-sharing websites (such as torrents) to download material from the internet, such as music, videos, games or applications, unless you have been given specific permission to do so by a staff member or a member of the IT staff..
- You should be aware that all your access to the Internet, including the sites you visit, any material you download, and attempts to access blocked sites or to send inappropriate email are recorded in logs that are monitored by IT staff and/or teaching staff.

What Happens If You Breach the Cyber Safety & Acceptable Use Policy?

If you breach this policy, you will be subject to Heathfield High School's Behaviour Management Policy.

- Minor breaches of this policy may result in the suspension of your IT account for a period of up to two weeks. Repeated occurrences of a minor breach or breaches may result in the same consequences as a major breach.

- Minor breaches include, but are not limited to -
    - Eating or drinking in the IT areas.
    - Not placing bags on the bag racks supplied.
    - Inappropriate use of furniture.
    - The playing of computer games.
    - Sending emails that contain a common swear word or words.

Major breaches of this policy may result in the suspension of your IT account for a period of up to ten weeks, the recall of your laptop or removal of access for home use, and/or your suspension from school, along with consequences in line with Heathfield High School's Student Behaviour Management Policy.

- Major breaches include, but are not limited to -
    - Giving your password to another student to access the network.
    - Using another student's password to access the network.
    - Saving executable programs from any source on the network.
    - Using executable programs from any source, other than those programs installed on the network.
    - Use of abusive, sexist, racist or threatening language in any document or email.
    - Using excessive swear words or other inappropriate language.
    - Deliberately damaging any equipment, irrespective of the extent of damage.
    - Interfering with any network hardware or software.
    - Attempting to circumvent network security in any way.
    - Attempting to bypass the DECS proxy server, accessing the internet through a non-approved device, or accessing the internet through an anonymous proxy server.

- If you behave online in a manner that threatens the well-being of another child, student, parent or member of the school community, even if this occurs off-site and/or out of school hours, the Principal has the authority under Regulations pursuant to the Education Act 1972 to suspend or exclude you from attendance at school.

- If the Principal suspects an electronic crime has been committed, this will be reported to the South Australian Police Department (SAPOL). Where there is reasonable suspicion that evidence of a crime, such as an assault, is contained on a mobile phone or other electronic device such as a laptop, the device will be confiscated and handed to the investigating police officer. SAPOL will determine any further action.