THE HEIGHTS SCHOOL

Student ICT Acceptable Use Policy

Last Updated: 24/11/2016

Dear Parent/Caregiver,

The measures to ensure the cyber-safety of The Heights School are based on our core values. To assist us to enhance learning through the safe use of information and communication technologies (ICTs), we are now asking you to read this document. Rigorous cyber-safety practices are in place, which include cyber-safety policies for staff and students. Child protection education, such as the Keeping Safe child protection curriculum, includes information about remaining safe when using new technologies and is provided to all students.

The computer network, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs at The Heights School, and to the effective operation of the school. The ICT equipment is for educational purposes appropriate to this environment, whether it is owned or leased either partially or wholly by the school, and used on or off the site.

The overall goal of The Heights School is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The ICT Acceptable Use Policy includes information about your obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

Material sent and received using the network may be monitored, and filtering and/or monitoring software may be used to restrict access to certain sites and data, including e-mail. Where a student is suspected of an electronic crime, this will be reported to the South Australia Police. Where a personal electronic device such as a mobile phone is used to capture images of a crime, such as an assault, the device will be confiscated and handed to the police.

While every reasonable effort is made by The Heights School to prevent student's exposure to inappropriate content when using the school's online services, it is not possible to completely eliminate the risk of such exposure. In particular, The Heights School cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child.

Please contact your child's classroom teacher, year level leader or sub school leader, if you have any concerns about your child's safety in using the Internet and ICT equipment/devices.

Important terms:

'Cyber-safety' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.

'Cyber bullying' is bullying which uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as e-mail, chat room discussion groups, instant messaging, webpages or SMS (text messaging) - with the intention of harming another person.

'School and preschool ICT' refers to the school's or preschool's computer network, Internet access facilities, computers, and other ICT equipment/devices as outlined below.

'ICT equipment/devices' includes computers (such as desktops, laptops, tablets), storage devices (such as USB and flash memory devices, CDs, DVDs, iPods, MP3 players), cameras (such as video and digital cameras and 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.

'Inappropriate material' means 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 or preschool environment.

'E-crime' occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices for themselves and the people around them regardless of the time of day. Being cyber-safe is no exception and we invite you to discuss with your child the following strategies to help us stay safe when using ICT at school and after formal school hours.

School Username and Password:

- Students in years 4-12 are issued with a personal user name. Students should only login with their own username.
- Students are to keep their password secret and secure.
- Students are personally responsible for any and all use of the network, including the cost of printing, Internet access, email access and disk storage, or any internet activity that occurs using their user-name and password.
- If students suspect that someone else knows their login details, that matter must be reported immediately to ICT.

Personal or BYOD devices:

- Personal ICT related devices (including laptops, tablets, mobile phones etc) are brought in and used for school work-related purposes only.
- Instructions for joining personal devices are located on the Intranet.
- Help is available from ICT to assist students connecting their devices, however this is provided on a best-effort basis.
- Pre-existing issues (such as hardware incompatibility, software related problems, malware etc) preventing devices being joined to the network are the responsibilities of the owner of the devices.
- All personal devices joined to The Heights School network, must have antivirus and security updates installed.
- All privately owned ICT equipment/devices (including laptops, tablets, mobile phones or any electronic storage device etc) that are brought into school or a school related activity are also covered by the ICT Acceptable Use Policy. Any images or material on such equipment/devices must be appropriate to the school environment.
- The school reserves the right to inspect personal/parent-owned ICT devices (including laptops, tablets, mobile phones or any electronic storage device etc) brought into school and confiscate such devices suspected of containing inappropriate material.

Mobile Phones:

- The use of mobile phones is permitted during times agreed to by the school and/or teacher during the school day.
- Mobile phones are not to be used to phone or text parents/caregivers as an alternative to school sign-in / sign-out policies.

Use of ICT equipment and online behaviour:

- While at school or a school related activity, any ICT material or activity that might put themselves or anyone else at risk (eg bullying or harassing), must be reported to a teacher.
- The use of the Internet, e-mail, mobile phones or any ICT equipment is for positive purposes only, 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.
- Students must not use any devices (including laptops, tablets, mobile phones, cameras etc) in an illegal or harassing manner. This includes taking photos or videos of any person without their permission, taking offensive photos or making sound recordings or videos etc.
- The use of the Internet shall only be performed through the school's filtered internet connection. At no point will a "personal hotspot" or mobile internet service be used.
- While at school, students will:
    - access, attempt to access, download, save and distribute only age appropriate and relevant material
    - report any attempt to get around or bypass security, monitoring and filtering that is in place at school.
- If students accidentally access inappropriate material, they need to:
    - not show others
    - turn off the screen or minimise the window
    - report the incident to a teacher immediately.
- Downloading or copying files such as music, videos, games or programs may only occur with the permission of a teacher or the owner of the original material. Students may be personally liable if they infringe the Copyright Act 1968. This includes downloading such files as music, videos, games and programs.

- The LearnLink Office 365 Service, including Office 365 Pro Plus is only to be used in relation to delivering curriculum objectives, and will not be used to store sensitive or personal information.
- Students must seek their teacher's permission before putting any personal information online. Personal identifying information includes any of the following:
    - full name
    - address
    - e-mail address
    - phone numbers
    - photos
- 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 e-mail.
- The school may monitor and 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 e-mail.
- All ICT equipment/devices/services provided by The Heights School must be respected and treated with care. This includes:
    - not intentionally disrupting the smooth running of any school ICT systems
    - not attempting to hack or gain unauthorised access to any system
    - following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with ICT
    - reporting any breakages/damages to a staff member.

Students responsibilities include:

- reading this ICT Acceptable Use Policy carefully
- following this policy and cyber-safety strategies whenever using the school's ICT facilities
- following this policy and cyber-safety strategies whenever using privately-owned ICT devices on the school site or at any school related activity, regardless of its location
- avoiding any involvement with material or activities that could put at risk personal safety, or the privacy, safety or security of the school or other members of the school community
- taking proper care of school ICT facilities. Families may have responsibility for the cost of repairs or replacement for students involved in the damage, loss or theft of ICT equipment/devices.
- keeping this document somewhere safe so it can be referred to it in the future
- asking the class teacher or year level leader if unsure about anything relating to this policy.

If any student is found to breach the ICT Acceptable Use Policy, the school may inform parents/caregivers. In serious cases, the school may take disciplinary action against a student. Families may be charged for repair costs. If illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform the police and hold securely personal items for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.