NURIOOTPA HIGH SCHOOL

Penrice Road, Nuriootpa South Australia 5355

Tel: (08) 8562 2022 Fax: (08) 8562 1029
Email: dl0788.admin@schools.sa.edu.au
Website: www.nurihs.sa.edu.au

Through adversity to the stars

TRADITION • RELATIONSHIPS • EXCELLENCE

ICT CYBER-SAFETY USER AGREEMENT POLICY

(Includes information and reference to Learnlink Office 365)

Dear Student and Parent/Caregiver,

The measures to ensure the cyber-safety of NURIOOTPA HIGH 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 and **sign** the **Nuriootpa High School ICT Acceptable User Agreement** (*refer separate document*) to signal your agreement to adhere to this Policy's terms as part of the annual enrolment process.

Rigorous cyber-safety practices are in place, which include cyber-safety Use Agreements for staff and students, who have been involved in the development of the agreement. 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 NURIOOTPA HIGH 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 NURIOOTPA HIGH SCHOOL is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The Use Agreement 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.

All students enrolled at NURIOOTPA HIGH SCHOOL are required to read and comply with the contents of this **NHS ICT Cyber-safety Policy** and once signed consent has been returned to school via the Nuriootpa High School ICT Acceptable User Agreement (*refer separate document*), students will be able to access and use the school ICT equipment and Internet and have full access to the NEW DECD Learnlink Office 365 online tools released at the beginning of 2017. Please refer to the separate information included in this Policy concerning Office 365 (*refer Page 3*).

Material sent and received using the school Curriculum and Internet networks, including 'online' Office 365, is monitored and filtering and/or monitoring of software may be used to restrict access to certain sites and data, including e-mail and Cloud storage. Where a student is suspected of an electronic crime, this will be reported to South Australia Police (SAPOL). Where a personal electronic device such as a mobile phone or laptop is used to capture images of a crime, such as an assault, the device will be confiscated and handed to SAPOL. It is a DECD requirement that portable USB devices, tablets, laptops, netbooks, iPads and mobile phone varieties used at school only contain educational files relevant to the student Curriculum being studied and that all files generated at or for school, remains the property of the Department of Education and Child Development. Files of this nature can be shared/distributed through the Office 365 Cloud, however, storage and/or sharing of non-curricular files, documents, images, games, movies will result in school disciplinary action.

While every reasonable effort is made by schools and DECD administrators to prevent student's exposure to inappropriate content when using the department's online services, it is not possible to completely eliminate the risk of such exposure. In particular, DECD cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. DECD recommends the use of appropriate Internet filtering software.

More information can be found on the following websites

- Department for Education and Child Development (DECD) - https://www.decd.sa.gov.au/supporting-students/health-e-safety-and-wellbeing/cyber-safety-bullying-and-harassment
- Australian Communications and Media Authority at http://www.acma.gov.au,
- NetAlarmed at http://www.netalarmed.com/
- Kids Helpline at http://www.kidshelp.com.au
- Bullying No Way at http://www.bullyingnoway.com.au.

Please contact the Principal, if you have any concerns about your child's safety in using the Internet and ICT equipment/devices.

Continued next page…

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 ICT' refers to the school's computer network, Internet access facilities, computers, and other ICT equipment/devices as outlined below.
'ICT equipment/devices' includes computers (such as desktops, laptops, iPads, PDAs), 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.

Strategies to help keep NURIOOPTA HIGH SCHOOL Students Cyber-safe

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.

1. I will not have access to school ICT (or Internet facilities) equipment until my parents/caregivers and I have signed my Use Agreement Form and the completed form has been returned to I.T. Services (T6 Office) at NURIOOTPA HIGH SCHOOL.
2. When I am allocated my own user name, I will log on only with that user name.
   I will not allow anyone else to use my log-on details or internet username and password.
3. I will keep my password private.
4. While at school or during a school related activity, I will inform the teacher of any involvement with any ICT material or activity that might put me or anyone else at risk (e.g. bullying or harassing).
5. I will use the Internet, e-mail, Microsoft Cloud, Google Apps for Education platform, mobile phones or any ICT equipment only for positive purposes, not to be mean, rude or offensive, or to bully, video someone, harass, or in any way harm anyone else, or the school itself, even if it is meant as a joke.
6. I will only use ICT devices to file share Curriculum based files, excluding games and other non-curricular files
7. I will use my mobile phone / electronic device (includes iPads, iPods, Tablets, DS, laptops) only at the times agreed to by the school during the school day.
   While at school, I 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.
8. If I accidentally access inappropriate material, I will:
   - not show others
   - turn off the screen or minimise the window
   - report the incident to a teacher immediately.
9. To ensure my compliance with copyright laws, I will download or copy files such as music, videos, games or programs only with the permission of a teacher or the owner of the original material. If I infringe the Copyright Act 1968, I may be personally liable under this law. This includes downloading such files as music, videos, games and programs.
10. My privately owned ICT equipment/devices, such as a laptop, tablet, iPad, mobile phone, or USB/portable drive I bring to school or use in a school related activity, also is covered by the Use Agreement. Any images or material on such equipment/devices must be appropriate to the school environment and if not, then immediately removed.
11. I will ask my teacher's permission before I put any personal information online. Personal identifying information includes any of the following:
    - my full name
    - my address
    - my e-mail address
    - my phone numbers
    - photos of me and/or people close to me.
12. I will respect all school ICTs and will treat all ICT equipment/devices 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 ICTs
    - reporting any breakages/damage to a staff member.

13. 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.
14. The school and/or the Department for Child Development 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.
15. If I do not follow cyber-safe practices, the school may inform my parents/caregivers. In serious cases, the school may take disciplinary action against me. Such actions may occur even if the incident occurs off-site and/or out of school hours.
16. If any materials or activities are involved which creates a suspicion on reasonable grounds that a child has been abused or neglected, the school may report these concerns to child protection authorities. Such actions may occur even if the incident occurs off-site and/or out of school hours.
17. If illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform SAPOL 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.

Learnlink Office 365 (DECD parent/guardian information)

NURIOOTPA HIGH SCHOOL has expanded the current LearnLink email service offered to students with additional services, and it is known as LearnLink Office 365 (*refer NHS website* - http://www.nurihs.sa.edu.au/office365.htm).

The services lets students download and use licenced versions of common Office applications for now charge. It also gives them their own storage space to share files with other students and their teachers whilst their student remains enrolled at NURIOOTPA HIGH SCHOOL.

Below is some important information from DECD regarding the LearnLink Office 365.

What is LearnLink Office 365?

LearnLink Office 365 is a customised package of Microsoft Office 365, tailored for the South Australian public education system. It includes several services and applications.

- **Email (existing service)**
  Students are provided a unique email address that remains the same throughout a student's enrolment in a State Government school or preschool.

- **Office 365 ProPlus (new)**
  Office 365 ProPlus lets Office applications be downloaded and installed on up to 5 personal devices owned by students (including parent-owned devices).
  Office applications that can be installed include Word, Excel, PowerPoint, OneNote, Access, Publisher and Outlook, however not all Office applications are available for Mac, iOS and Android devices.

- **Office Online (new)**
  Office Online is a web based, lightweight version of Microsoft's Office productivity suite (including Word, PowerPoint, Excel, and OneNote) that can be used on most devices capable of connecting to the internet via a web browser.

- **OneDrive for Business (new)**
  OneDrive for Business is a cloud service where students can store, sync, update, and share files from any internet connected web-browser, and collaborate on Office documents.

  Each student receives 1 Terabyte (or 1000 Gigabytes) of storage space in the cloud. By default all data and files are private, however students can choose to share files with other LearnLink Office 365 users, including staff and students of other schools and preschools. Sharing with anyone external to DECD schools/preschools will not be possible.

Using LearnLink Office 365 Services

All students are required to sign conditions of use agreements before they have access to school computers, internet, and software which outlines acceptable use.

The acceptable use agreements have been updated to outline conditions of use for the additional LearnLink Office 365 services.

A number of services provided by LearnLink Office 365 require internet access.

When students are onsite at NURIOOTPA HIGH SCHOOL, internet access will be filtered by DECD, however, access from home/off-site is not filtered by DECD and as such should be supervised.

Please be aware that as with any internet use, it is possible (that viruses and/or other malicious software could be introduced to your personal computing devices.

It is strongly recommended that personal devices have their operating system, suitable anti-virus / anti-malware software installed and it is regularly updated.

Users of LearnLink Office 365 are responsible for the information/data in their LearnLink Office 365 account and any important information should be backed up. LearnLink Office 365 including Office 365 ProPlus is only to be used in relation to delivering curriculum objectives, and must not be used to store, transmit or share sensitive personal information.

Installing Office 365 ProPlus

Office 365 ProPlus applications will need to be installed on a computer or mobile device (personal device) before it can be used.
It is possible that installing Office 365 ProPlus on your personal device may cause problems, such as conflicts with other software you have installed.

It is recommended that you:

- Backup your personal device, prior to installing Office 365 ProPlus application(s); and
- Ensure your personal device meets or exceeds the Office 365 System Requirements https://products.office.com/en-au/office-system-requirements.

What if I do not want my child(ren) to use the LearnLink Office 365 Services?

NURIOOTPA HIGH SCHOOL requires written notification by the end of February each calendar year if you do not consent to your child(ren) using the additional LearnLink Office 365 Services.
Please email the Digital Technologies Coordinator – john.barkley601@schools.sa.edu.au

| **Cyber-Safety: Keeping Children Safe in a Connected World** | June 2009 |

The below information comes from Page 15 of the "Keeping Children Safe in a Connected World" Policy document issued by the Department of Education and Child Development – June 2009.

Appropriate Behaviour and Use

DECS ICT Security, Internet Access and Use, and Electronic Mail and Use policies contain the following main provisions.
• Children and students may use the Internet only for learning related activities that are approved by a teacher. They must not cause interference or disruption to other people or equipment, and children may not access or distribute inappropriate material.
This includes:

- distributing spam messages or chain letters
- accessing or distributing malicious, offensive or harassing material, including jokes and images
- bullying, harassing, defaming or giving offence to other people
- spreading any form of malicious software (eg viruses, worms)
- accessing files, information systems, communications, devices or resources without permission
- using for personal financial gain
- using non-approved file sharing technologies (eg Torrent)
- using for non-educational related streaming audio or video
- using for religious or political lobbying
- downloading or sharing non-educational material.

All children and students must have annual access to developmentally appropriate child protection curriculum.

Recommendations - Good Practice Advice

Educators should:

- teach topics and use resources contained in the Keeping Safe: Child Protection Curriculum introduced to preschools and schools in 2008
- encourage children and students to inform a teacher if they come across inappropriate material or anything online that makes them feel uncomfortable
- teach strategies to manage online presence, protect identity through privacy settings, examine 'terms and conditions' associated with user agreements of Internet services, highlight the opportunities to report abuse or offensive online behaviour to the appropriate service provider or authority
- teach children and students (in an age appropriate way) how to identify and avoid inappropriate materials.

These can include:

- pornography - both illegal and legal pornography. It is prevalent on the Internet and can be accessed through websites, sent as spam via e-mails, shared in peer-to-peer networks or sexting through mobile phone messaging
- hate groups - including racial, religious, political, homophobic and other groups that are discriminatory
- violence or illicit drugs - websites containing explicitly violent behaviour (like rape or assault), material regarding illicit drugs or inciting suicide, vigilante or violent groups' websites, and instructional websites (like weapon or bomb making)
- illegal activity - content that promotes illegal activity (like copyright infringement on music), security breaches (like hacking) or fraudulent schemes online
- extremist groups and cults - groups online that offer information about their extremist or cult activities, goals and missions; these groups can use the Internet to recruit new members or incite action
- social networking - many social networking sites place children and students at some risk through exposing their identity, invading privacy and providing opportunities for bullying
- online advertising - some online advertising can be inappropriate for children and students; the Internet is an inexpensive medium for advertisers and is therefore widespread
- online gambling - websites which contain and promote gambling practices.

The entire DECD Cyber-safety Policy document (23 pages) can be downloaded from the internet via…
decd.sa.gov.au/docs/documents/1/cybersafetykeepingchildre.pdf

---

ICT CYBER-SAFETY POLICY SUMMARY

To the parent/caregiver/legal guardian and student:

Please ensure you have read this document carefully to ensure that you understand your responsibilities under this Policy Agreement.

I understand that NURIOOTPA HIGH SCHOOL will:

- Do its best to enhance learning through the safe use of ICTs. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or on school ICT equipment/devices at school, or at school related activities; and enforcing the cyber-safety requirements detailed in Use Agreements
- Respond to any breaches in an appropriate manner
- Provide members of the school community with cyber-safety education designed to complement and support the Use Agreement initiative
- Welcome enquiries at any time from parents/caregivers/legal guardians or students about cyber-safety issues.

For the Student: My responsibilities include…

- Reading this Cyber-safety Use Agreement carefully
- Following the cyber-safety strategies and instructions whenever I use the school's ICTs
- Following the cyber-safety strategies whenever I use 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 my own safety, or the privacy, safety or security of the school or other members of the school community
- Taking proper care of school ICTs. I know that if I have been involved in the damage, loss or theft of ICT equipment/devices, I and/or my family may have responsibility for the cost of repairs or replacement
- Keeping this document somewhere safe so I can refer to it in the future
- Asking the [relevant staff member] if I am not sure about anything to do with this agreement.

…Continued Page 6

For the Parent/Caregiver/Legal Guardian: My responsibilities include…

- Reading this ICT Cyber-safety Use Agreement carefully and discussing it with my child(ren) so we both have a clear understanding of our roles in the school's work to maintain a cyber-safe environment
- Ensuring the Nuriootpa High School ICT Acceptable User Agreement – Student Version is signed by my child and by me and returned to the school
- Encouraging my child to follow the cyber-safe strategies and instructions
- Adhering to the terms of this agreement, and supporting steps taken by the school ensure compliance
- Contacting the school if there is any aspect of this ICT Cyber-safety Use Agreement I would like to discuss.

Please note: This agreement will remain in force for as long as your child is enrolled at Nuriootpa High School.
If it becomes necessary to add/amend any information or rule, you will be advised in writing.

Please refer to the **Nuriootpa High School ICT Acceptable User Agreement**,
which MUST be signed and returned to the Digital Technologies Coordinator
prior to NHS ICT access being provided