GAWLER & DISTRICT COLLEGE B-12

2018 Cyber-Safety Use Agreement Year 7 to Year 12

Dear Parent/Caregiver,

The measures to ensure the cyber-safety of Gawler & District College B-12 are based on our core values of Respect, Generosity and Excellence. 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 attached Use Agreement Form.

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 Gawler & District College B-12, 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 Gawler & District College B-12 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 will be issued with a Cyber-Safety Use Agreement and once signed consent has been returned to school, students will be able to use the school ICT equipment.

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 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 about Internet filtering can be found on the websites of the Australian Communications and Media Authority at http://www.acma.gov.au, NetAlert at http://www.netalert.gov.au, the Kids Helpline at http://www.kidshelp.com.au and Bullying No Way at http://www.bullyingnoway.com.au.

Please contact the relevant Middle or Senior 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, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, 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 Gawler & District College B-12 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 use school ICT equipment only when my parents/caregivers have signed my Use Agreement form and the completed form has been returned to school.

2. I will use the computers and other ICT equipment only for research and tasks that are related to my school work.

3. I will log on only with my own user name and password. I will not allow anyone else to use my logon details.

4. I will keep my password private.

5. While at school or 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 (eg bullying or harassing).

6. I will use the Internet, e-mail, or any ICT device only 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.

7. I will go online or use the Internet at school only when a teacher gives permission.

8. While at school, I will:
    - attempt to access, access, download, save and distribute only age appropriate and material relevant to my school work.
    - report any attempt to get around or bypass security, monitoring and filtering that is in place at school.

9. No executable files (.exe file), or any other inappropriate files, including computer games, pornography, music, movies and images not used for school work, are to be stored in students directories or brought to school on a usb or any other device.

10. 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.

11. 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.

12. My privately owned ICT devices that I bring to school or for a school related activity, is also covered by this Cyber-Safety Use Agreement. Any images, apps or files on such equipment/devices must be appropriate to the school environment.

13. Only with written permission from the teacher will I connect any ICT device to school ICT, or run any software - this includes all wireless/Bluetooth technologies.

14. 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, others and/or people close to me.

15. I will respect all school lCTs 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
    - not seeking information on how to disrupt school or any other ICT services
    - not encouraging others to use ICTs inappropriately
    - 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.

16. The school may monitor traffic and files 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.

17. 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.

18. 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. My family 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.

19. 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.

2018 Cyber-Safety Use Agreement Form – Year 7 to 12

To the parent/caregiver/legal guardian:

Please read this page carefully to check that you understand your responsibilities under this agreement.

Return the signed Use Agreement to the school.

I understand that Gawler & District College B-12 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
- work with children and their families to encourage and develop an understanding of the importance of cyber-safety through education designed to complement and support the Cyber-Safety Use Agreement initiative. This includes providing children with strategies to keep themselves safe in a connected online world
- respond to any breaches of this agreement in an appropriate manner
- 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 a copy of this document somewhere safe so I can refer to it in the future
- asking my home care teacher if I am not sure about anything to do with this agreement.

PLEASE COMPLETE THE REPLY SLIP BELOW, CUT OFF AND RETURN TO SCHOOL.
KEEP THE ABOVE INFORMATION FOR YOUR OWN REFERENCE.

✂----------

2018 CYBER-SAFETY USE AGREEMENT – YEAR 7 TO 12

We have read and understood this Cyber-safety Use Agreement and we are aware of the school's initiatives to maintain a cyber-safe learning environment.

Print Name of student.....Student Id No. .....

Year Level..... Home Care .....

Signature of student..... Date.....

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

- reading this Cyber-safety Use Agreement carefully and discussing it with my child so we both have a clear understanding of our roles in the school's work to maintain a cyber-safe environment
- ensuring this Use Agreement is signed by my child and by me and returned to the school
- encouraging my child to follow the cyber-safe strategies and instructions
- contacting the relevant Sub-School Leader if there is any aspect of this Use Agreement I would like to discuss.

Print name of parent/caregiver/legal guardian.....

Signature of parent/caregiver/legal guardian..... Date.....

FOR ICT OFFICE USE:

☐ DAYMAP ☐ ACTIVE DIRECTORY (ID No. (Initials) & Email) ☐ CUA DATABASE

☐ LEARNLINK ☐ LYNDA.COM ☐ MATHLETICS ☐ MOODLE

ENTERED DATE ……/……/……. BY ……