Cyber Safety Policy

Rationale
Mannum Community College places a high priority on providing its school community with Internet facilities, ICT devices and equipment which will benefit student learning outcomes and the effective operation of the school.

Mannum Community College recognises that the presence in the learning environment of these technologies (those provided by the school and some privately owned by staff, students or other members of the school community), can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximise the benefits of these technologies, whilst at the same time minimise and manage the associated risks.

Mannum Community College thus acknowledges the need to have in place rigorous and effective cyber-safety practices which are directed and guided by this cyber-safety policy.

Aims
- To develop and maintain rigorous and effective cyber-safety practices which aim to maximise the benefits of the Internet and ICT devices / equipment to student learning.

- The effective operation of the school, while minimising and managing risks.

- To address the need of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.

Implementation
Mannum Community College’s cyber-safety practices are to be based on information contained in the latest versions of DECD Policies.

No individual may use the school Internet facilities and the school – owned/ leased ICT devices / equipment in any circumstances unless the appropriate Cyber-safety Agreement has been signed and returned to the school. Cyber-safety Agreements also apply to the use of privately – owned / leased / or issued from other workplace; devices and equipment on the school site, or at / for any school related activity, regardless of its location. This includes off site access to the school network from school or privately – owned / leased equipment.

Mannum Community College Cyber-safety Agreements will cover all staff, students and any other individuals authorised to make use of the school internet facilities and ICT devices / equipment, such as pre-service teachers, external tutors and providers, contractors and other visitors to the school.

Cyber-safety Agreements are also an educative tool and shall be used as a resource to support the professional development of the school community.
Use of the Internet and the ICT devices / equipment by staff, students and other approved users at Mannum Community College is to be limited to educational, professional development and personal usage appropriate in the school environment, as defined in Cyber-safety Agreements.

Signed Cyber-safety Agreements will be filed in a secure place and an appropriate system devised which facilitates confirmation that particular individuals are authorised to make use of the Internet and ICT devices / equipment.

Mannum Community College has the right to monitor access and review all use. This includes personal emails sent and received on the school’s computer/s and / or network facilities at all times.

Mannum Community College has the right to audit at any time any material on equipment that is owned or leased by the school.

At Mannum Community College the safety of students is of paramount concern. Any apparent breach of the Cyber-safety Policy and /or the Harassment Policy will be taken seriously. All disciplinary responses need to be appropriate to the level of severity of the breaches of the Mannum Community College Cyber-safety Policy and/or Harassment Policy

The response to individual incidents will follow the procedures developed as part of the school’s Cyber-safety practices and/or Harassment procedures. In serious incidents advice will be sought from an appropriate source. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

There will be need for on-going funding for Cyber-safety practices through inclusion in the global budget.

Mannum Community College will provide ongoing professional training and development regarding the embedding of Cyber-safety into the curriculum. The knowledge base of all members of the school community will be maintained with the distribution of up-to-date information.

All care group programs (R-12) will include a unit of work on Cyber-safety, specifically designed to cater for the needs of each year level group. This will be reviewed annually to keep all information correct and up to date.

All members of the Mannum Community College community will be educated regarding their role in maintaining a cyber-safe, wider school community.

All members of the school community will be educated regarding the implications of their “digital footprint” and the implications for potential employment and community issues.

Evaluation
This policy will be reviewed in 2018
Note: Attached Cyber-safety User Agreements for Primary/Middle Years Students and Secondary Years Students.
CYBER-SAFETY AT MANNUM COMMUNITY COLLEGE – PRIMARY/MIDDLE YEARS R-7

Dear Parent/Caregiver,

The measures to ensure the cyber-safety of Mannum Community College 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 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 Mannum Community College, 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 Mannum Community College 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 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 DECS administrators to prevent children’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, DECS cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. DECS recommends the use of appropriate Internet filtering software.


Please contact the principal, 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 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, 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.
Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child’s safety and safe practices 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 use school ICT equipment until my parents/caregivers and I 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 my learning.

3. I will go online or use the Internet at school only when a teacher gives permission and an adult is present.

4. If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.

5. If I have my own user name, I will log on only with that user name. I will not allow anyone else to use my name.

6. I will keep my password private.

7. I will use the Internet, e-mail, mobile phones or any ICT equipment 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.

8. While at school, I will:
   • attempt to search for things online that I know are acceptable at our school. This would exclude anything that is rude or violent or uses unacceptable language such as swearing
   • report any attempt to get around, or bypass, security, monitoring and filtering that is in place at our school.

9. If I find anything that upsets me, is mean or rude, or that I know is not acceptable at our school, I will:
   • not show others
   • turn off the screen
   • get a teacher straight away.

10. Only with written permission from home and the school will I bring any ICT equipment/devices to school. This includes things like mobile phones, iPods, games, cameras, and USB/portable drives.

11. Only with written permission from the teacher will I connect any ICT device to school ICT, or run any software (eg a USB/portable drive, camera or phone). This includes all wireless/Bluetooth technologies.

12. The school cyber-safety strategies apply to any ICTs brought to school.

13. To ensure my compliance with copyright laws, I will download or copy any files such as music, videos, games or programs only with the permission of a teacher or the owner of the original material.

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 and/or people close to me.

15. 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.

16. If I do not follow cyber-safety 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.
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 Mannum Community College 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 ICT equipment/devices at school or at school-related activities
• 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 Use Agreement initiative. This includes providing children with strategies to keep themselves safe in a connected online world
• respond to any breaches in an appropriate manner
• welcome enquiries at any time from parents/caregivers/legal guardians or children about cyber-safety issues.

My responsibilities include:

• discussing the information about cyber-safety with my child and explaining why it is important
• supporting the school’s cyber-safety program by emphasising to my child the need to follow the cyber-safety strategies
• contacting the principal or nominee to discuss any questions I may have about cyber-safety and/or this Use Agreement.

---------------------------------------------

CYBER-SAFETY USE AGREEMENT

I have read and understood this Cyber-safety Use Agreement and I am aware of the school’s initiatives to maintain a cyber-safe learning environment.

Name of child...........................................................................................................................................................................

Group/Class .............................................................................................................................................................................

Name of parent/caregiver/legal guardian.........................................................................................................................

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

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

PLEASE RETURN THIS SECTION TO SCHOOL AND KEEP A COPY FOR YOUR OWN REFERENCE.
Dear Parent/Caregiver,

The measures to ensure the cyber-safety of Mannum Community College 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 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 Mannum Community College, 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 Mannum Community College 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 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 DECS 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, DECS cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. DECS recommends the use of appropriate Internet filtering software.


Please contact the principal, 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 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, 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.
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 use school ICT equipment until my parents/caregivers and I have signed my Use Agreement Form and the completed form has been returned to school.

2. If I have my own user name, I will log on only with that user name. I will not allow anyone else to use my name.

3. I will keep my password private.

4. 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).

5. I will use the Internet, e-mail, mobile phones or any ICT equipment 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.

6. I will use my mobile phone/s only at the times agreed to by the school during the school day.

7. I will go online or use the Internet at school only when a teacher gives permission and an adult is present.

8. 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.

9. 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.

10. 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.

11. My privately owned ICT equipment/devices, such as a laptop, mobile phone, USB/portable drive I bring to school or 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.

12. Only with written permission from the teacher will I connect any ICT device to school ICT, or run any software (eg a USB/portable drive, camera or phone). This includes all wireless/Bluetooth technologies.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.
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 Mannum Community College 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.

---

CYBER-SAFETY USE AGREEMENT

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.

Name of student........................................................................................................ Group/Class ........................................

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 school if there is any aspect of this Use Agreement I would like to discuss.

Name of parent/caregiver/legal guardian........................................................................................................

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

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

PLEASE RETURN THIS SECTION TO SCHOOL AND KEEP A COPY FOR YOUR OWN REFERENCE.