POLICY:	**Computer Acceptable Use Policy**
DATE:	November 2019
ENDORSED BY COLLEGE COUNCIL:	28 November 2019
TO BE REVIEWED:	28 November 2022

Introduction

This policy sets out the rights and regulations governing access to network and internet resources.

Parents/Carers and students are required to sign the agreement upon enrolment at Strathmore Secondary College [SSC]. Students are provided with a unique login, school email address and password upon commencement.

Access to the internet for educational purposes is a privilege. SSC provides a filtered wireless network through the Department of Education and Training (DET) internet service provider. The college uses software that is able to identify individual users on the network. If a student believes the security of their password has been compromised, they should contact the Information Technology (IT) Office (B Corridor) immediately.

User Responsibilities

- Students should keep their password safe and secure. Under no circumstances should any student divulge their password to someone else.
- Students are responsible for their own folders (including their Google Drive), network share areas, printing, passwords, equipment and information accessed and sent online (both within and outside the school's computer network).
- Only school work related material should be saved in student folders (Google Drive and Server Drive).
- Students should remove material that is no longer needed from their personal network drives. Folder contents will be deleted at the conclusion of each school year.

Appropriate Use

- When communicating through the internet or email, students are required to behave in a responsible and courteous manner.
- Students should will only access material that is relevant to their work and respect the ownership of material created by others.

Inappropriate Use

The following is a list of practices that are considered inappropriate. While this list is extensive, it is not exhaustive.

Students will not engage in the following behaviour:

- Use of the network for unsanctioned commercial purposes or the display of advertisements.
- Use of the network to disrupt its use by others.
- Violation of copyright laws.
- Use of personal web pages to conduct political lobbying or to vilify others.

- Creating hyperlinks to sites that contain material that is contrary to SSC policy.
- Provide false or misleading information through e-mail or internet communications.
- Email spamming, flaming or the distribution of junk mail.
- Students will not participate in online gaming while connected to the college network.
- Students will not install or use peer to peer programs e.g. Bit Torrent, uTorrent.
- Students will not use chat programs e.g. iMessage, FaceTime, Skype unless directed by teachers for curriculum purposes.
- Students will not use social media
- Students will not install or use Virtual Private Network Apps or Programs on any devices.

Network Security and Possession of Inappropriate Material

Any data stored in network folders is covered by the same rules that govern any other physical possession owned by a student. Where students have or are suspected of possessing inappropriate material, staff may confiscate the storage media for review. The IT Manager or IT staff may also access share areas to determine if rule breaches have occurred or to ensure that system integrity is being maintained. Files that are found in a user's area that are deemed to be inappropriate or that threaten network security or integrity may be deleted and further action may be taken.

Sanctions

Depending on the severity of the nature of the rule breeches, damage or inconvenience created, the following sanctions may occur:

- Suspension of user accounts
- Withdrawal of network privileges including online access
- Detentions
- Paying for replacement of damaged hardware, including network cabling and components
- Paying a service fee for the time involved in repairing software damage

Serious breaches may involve other school based sanctions such as suspensions, expulsions, and the involvement of external agencies such as law enforcement agencies.

Student Internet Acceptable Use Agreement

When accessing the Internet at Strathmore Secondary College, I agree to:

- protect my privacy rights and those of other students by not giving out personal details including full names, telephone numbers, addresses and images
- use the Internet in line with my school's student code of conduct and use appropriate language when talking to and working with others online and never participate in on line activity that harasses or hurts others
- use the Internet at SSC for educational purposes and use the equipment properly
- **NOT** use social media
- not deliberately enter or remain in any site that has obscene language or offensive content (e.g. racist material or violent images)
- abide by copyright procedures when using content on websites (ask permission to use images, text, audio and video and cite references where necessary)
- think about how I use content posted on the Internet and not simply copy and paste information from websites
- not interfere with network security, the data of another user or attempt to log into the network with a user name or password of another student
- not reveal my password to anyone except the system administrator, classroom teachers or student coordinators

- not bring or download unauthorised programs, including games, to the school or run them on any devices connected to the school network
- talk to my teacher or another adult if:
    - I need help online
    - I feel that the welfare of other students at the school is being threatened by online activities
    - I come across sites which are not suitable for our school
    - Someone writes something I don't like, or makes me and/or my friends feel uncomfortable or asks me to provide information that I know is private.

I have read the Internet Acceptable Use Agreement carefully and understand the significance of the conditions and agree to abide by these conditions. I understand that any breach of these conditions will result in my Internet access privileges being suspended or revoked.

Student Name: ……

Year Level: ……

Student Signature: ……

Parent/Carer Signature:

Date: ……

Information for Parents/Carers

Strathmore Secondary College (SSC) uses the Internet as a teaching and learning tool. We see the Internet as a valuable resource, but acknowledge it must be used responsibly.

Your child has been asked to agree to use the Internet responsibly at school. Parents/Carers should be aware that the nature of the Internet means that full protection from inappropriate content can never be guaranteed.

At **SSC** we:

- provide a filtered service
- provide access to the Victorian Education Channel -www.education.vic.gov.au/secondary/, a search engine that can be used to control student access to websites that have been teacher recommended and reviewed
- provide supervision and direction in Internet activities
- work towards setting tasks that ask students open questions, so they don't simply copy and paste all answers from the Internet
- reinforce the importance of safe and respectful use of the Internet.

Bridging the gap between home and school

At SSC the Internet is mostly used to support teaching and learning. At home, however, it is often used differently. Not only is it a study resource for students, but it is also used as a social space to meet and chat.
If you have the Internet at home, encourage your child to show you what they are doing online.

At home we recommend you follow these Top Ten Tips from the Alannah & Madeline Foundation (2019):

1. Create an 'Acceptable Use Agreement' for your families to facilitate conversation. Ensure that children are involved with this process.
2. Set up safe search & security controls with a platform such as Family Zone www.familyzone.com/au/
3. Agree on where computers, laptops & mobile devices can be used in the home (such as in bedrooms, lounge rooms, etc.)
4. Lights out = Wi-Fi off.
5. Agree on screen time use; decide on 'screen free' times during the day and night. Have regular family activities that don't involve devices.
6. Get involved – show an interest in what your child is doing online.
7. Talk to your child's teacher/s and school.
8. If your child reports an issue to you, don't threaten to take away their device – this may force them to become secretive.
9. Learn how various social network/game services work. Use websites such as the 'Games, Apps & Social Networking' from the eSafety Office.
10. If cyber bullied;
    1. Don't retaliate
    2. Collect evidence
    3. Report
    4. Change privacy setting
    5. Block
    6. Tell a trusted adult.

What has your child agreed to and why?

Protecting personal privacy rights and those of other students

Some students like to publish information about themselves and their friends using social media apps. In doing so they can make themselves more vulnerable to being approached, groomed or bullied online. To avoid this, we recommend they:

- Don't share personal details including their name, images of themselves or their friends online
- Restrict privacy settings of social media accounts
- Password protect any spaces or accounts they have
- Don't allow anyone they don't know to join their chat or collaborative space
- Are reminded that any image or comment they put on the Internet is public (anyone can see, change or use it) so no full names should appear in reference to individuals in any image, movie or sound recording.

Using the Internet in line with SSC's Student Code of Conduct

Using appropriate language when talking to and working with others online and never write or participate in hate mail.

Being online can make students feel that they are anonymous and sometimes students may say things online that they would never say to someone's face. SSC encourages students to always be respectful and use appropriate language when communicating with anyone in person, or online.

Using equipment and resources properly for educational purposes as directed by teachers

Some students may often see the Internet as free but just looking at a page on the Internet incurs a download cost. By taking care with the equipment and thinking carefully about printing and downloading from the Internet students can save time, money and be environmentally responsible.

Keeping away from rude or offensive sites.

In school settings, DET and their Internet Service Provider set up filters to block out a lot of inappropriate content, but these filters are not foolproof. Students who deliberately seek out inappropriate content or use technology that bypasses filters will have their Internet access reviewed and their parents/carers will be informed.

Following copyright procedures

All content on the Internet is owned by someone. Many items are 'copyright' protected and breaking copyright is

breaking the law.
By downloading unknown software, you can also risk bringing a virus or spyware to the computer, device or system. These can destroy a computer system or provide hackers with details such as passwords and bank accounts.

Evaluating and using content on the Internet carefully
Not everything on the Internet is true, accurate or unbiased. The school is working to teach digital literacy skills, which enables students to locate, evaluate, and use information from the Internet effectively.
Copying and pasting information can help organise arguments, ideas, and information, but it is important that your child uses their own thoughts and language to express what they have learnt.

Not interfering with network security, the data of another user or attempt to log into the network with a user name or password of another student
Computer facilities are for the use of all students so due care should be taken at all times when using these resources. SSC students are responsible for everything done using their accounts, and everything in their home directories. To this end, students need to keep their password secret and not gain access to other students' login details.

Seeking teacher assistance
SSC students should ask for help in locating the information they need and clarifying tasks they have been set to complete. Unfocused clicking through websites can lead to inappropriate content.

We also want the school community to keep their Internet environment as safe as possible so we ask your child if they see a site they think should be blocked, to turn off their screen and let a teacher or trusted adult know.

Open communication between parents/carers, teachers and students is the best way to keep students safe.

If you have any concerns about this agreement or Internet Safety in general, contact either SSC or visit:

- Office of the eSafety Commissioner: www.esafety.gov.au
- iParent (eSafety Office): www.esafety.gov.au/education-resources/iparent
- Family Zone: www.fzo.io/amf
- Common Sense Media: www.commonsensemedia.org
- Video Games Advice: www.videogames.org.au

REVIEW PERIOD

This policy was last updated in November 2019 and is scheduled for review in November 2022.