Policy

Cyber Safety Policy

Summary

This policy sets out the framework, guidelines and obligations regarding Cyber Safety and acceptable use of technology at Seaford Secondary College.

Table 1: Document Details

Publication Date:	April 2020
Review Date:	April 2021
Replaces:	
Developed By:	Ben Hardy & ICT Governance Committee, in consultation with the Executive Leadership Team
Consultation:	Operational Leaders, staff, students, Governing Council
Approval By:	
Approval Date:	
Appendices:	
Version:	Version 2

Table of Contents

Policy **1**

Cyber Safety Policy **1**

Summary **1**

1. Title **3**

Cyber Safety Policy 3

2. Purpose **3**

3. Scope **3**

4. Policy Detail **4**

4.1 Students Expectations For Safe & Appropriate Use If ICT At Seaford Secondary College 4
4.2 Parent/Caregiver Responsibilities 5
4.3 Student Responsibilities 5
4.4 School Responsibilities 5
4.5 Responding To Breeches Of The Cyber Safety Policy 6
4.5.1 Classroom Teacher or Leader Identifies The Breech In The Cyber Safety Policy 6
4.5.2 House Leader Follow Up 6
4.5.3 It Team Follow Up 6
4.5.4 Principal Or Deputy Principal Follow Up 6

5. IMPORTANT INFORMATION FOR STUDENTS AND FAMILIES **6**

5.1 What is Cyber-Bullying 6
5.2 Important information for parents/caregivers 7
5.2.1 Signs that your child is being cyber bullied 7
5.2.2 What to do if your child is being cyber bullied 7
5.2.3 What to do if your child being a bully 8
5.3 Important Information for Students 9
5.3.1 What to do if you are being bullied 9
5.3.2 Impact of Bystanders; What to do if you see bullying towards others 9
5.3.3 Think about the impact of your actions on others 10

6. MONITORING, EVALUATION & REVIEW **10**

1. TITLE

Cyber Safety Policy

2. PURPOSE

Keeping students safe online is paramount. Students need to have safe conditions for learning to be successful, as well as build skills and knowledge to be safe and responsible global digital citizens.

3. SCOPE

The measures to ensure the cyber-safety of Seaford Secondary College are based on our core values: To assist us to enhance learning through the safe use of information and communication technologies (ICTs).

Rigorous cyber-safety practices are in place, which include cyber-safety User 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 technology.

The computer network, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs at Seaford Secondary 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 Seaford Secondary College is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The User Agreement includes information to all stakeholders about their obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breeches 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 Australian 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 Department for Education administrators to prevent students' 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, Department for Education cannot filter Internet content accessed by students from home, from other locations away from school or on mobile devices owned by students. Department for Education recommends the use of appropriate Internet filtering software for student owned devices out of school.

We also recommend that parents regularly monitor their child's use of technology, particularly internet and social media. It is also vital that parents are in regular communication with their child about acceptable use of technology to be safe and responsible digital citizens, as well as check on their wellbeing and that they are not a victim of online bullying.

More information about Internet filtering can be found on the websites of the Australian Communications and Media Authority at http://www.acma.gov.au, https://www.esafety.gov.au/ https://www.staysmartonline.gov.au/, the Kids Helpline at https://kidshelpline.com.au/ and Bullying No Way at http://www.bullyingnoway.com.au.

4. POLICY DETAIL

4.1 Students Expectations for Safe & Appropriate use if ICT at Seaford Secondary College

All students and parents/caregivers will sign an ICT User Agreement (see Appendix 1) before having access to any technology at Seaford Secondary College. It is expected that all students will comply with the ICT User Agreement at all times when using any form of technology at the school to ensure the safety of themselves & others. Failure to do so will lead to consistent responses in line with the school behaviour management policy including potentially (a) loss of computer access, (b) Time Out or suspension, (c) police action and confiscation of their digital device if deemed unlawful, (d) charge of repair costs to families for malicious or negligent damage. Student expectations for the safe use of ICT at Seaford Secondary College include:

1. Will not use school ICT equipment until a parent/caregiver and student have signed the Use Agreement Form and the completed form has been returned to school.
2. Log on only with their own user name and not allow anyone else to use their account.
3. Create a complex password and keep it private.
4. While at school or a school related activity, inform the teacher of any involvement with any ICT material or activity that might put them or anyone else at risk (eg bullying or harassing).
5. 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. Use their mobile phone/s only at the times agreed to by the school during the school day.
7. Go online or use the Internet at school only when a teacher gives direction.
8. While at school, students will:
    i. access, attempt to access, download, save and distribute only age appropriate and relevant material
    ii. report any attempt to get around or bypass security, monitoring and filtering that is in place at school
9. If students accidentally access inappropriate material, they must:
    i. not show others
    ii. turn off the screen or minimise the window
    iii. report the incident to a teacher immediately
10. To ensure student compliance with copyright laws, student 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 students infringe the Copyright Act 1968, they may be personally liable under this law. This includes downloading such files as music, videos, games and programs.
11. Student privately owned ICT equipment/devices, such as a laptop, mobile phone, USB/portable drive brought to school or a school related activity, are also covered by this User Agreement. Any images or material on such equipment/devices must be appropriate to the school environment.
12. Only with direction from the teacher will students 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. Follow all Cyber-Safety practices before putting any personal information online. Personal identifying information includes full name, address or phone number, e-mail address, photos of themselves and/or people close to them.
14. Respect all school lCTs and treat all ICT equipment/devices with care. This includes:
    i. not intentionally disrupting the smooth running of any school ICT systems
    ii. not attempting to hack or gain unauthorised access to any system
    iii. following all school cyber-safety strategies, and not join in if other students choose to be irresponsible with ICTs
    iv. reporting any breakages/damage to a staff member
15. Understand that 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. Understand that 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.

4.2 Parent/Caregiver Responsibilities

- Read the ICT User Agreement and Digital Learning Program Policy Document carefully and discuss it with their child so they have a clear understanding of their role in the school's work to maintain a cyber-safe environment
- Ensure the User Agreement is signed by the child and by the parent/caregiver and returned to the school
- Encourage their child to follow the cyber-safe strategies and instructions & report any bullying to a responsible adult
- Contact the school if there is any aspect of the User Agreement they would like to discuss
- Contact the school if there are any concerns over their child's safety or wellbeing related to cyber safety concerns, including harassment and bullying

4.3 Student Responsibilities

- Read the User Agreement & Digital Learning Program Policy Document carefully
- Follow the cyber-safety strategies and instructions whenever they use the school's ICTs and when on personal devices. This includes not bullying any students and report any bullying that is witnessed
- Follow the cyber-safety strategies whenever they use privately-owned ICT devices on the school site or at any school-related activity, regardless of its location
- Avoid any involvement with material or activities that could put at risk their own safety, or the privacy, safety or security of the school or other members of the school community
- Take proper care of school ICTs and understand that if there is evidence that they have caused damage, loss or theft of ICT equipment/devices, they and/or their family may have responsibility for the cost of repairs or replacement
- Keep the ICT User Agreement document somewhere safe to refer to it in the future
- Ask a relevant staff member if they are not sure about anything to do with the agreement.
- Report any actions of any other students who breech the ICT User Agreement, including cyber bullying.

4.4 School Responsibilities

- Enhance learning through the safe use of ICTs. This includes restricted 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 User Agreements
- Respond to any breeches in an appropriate manner, following the schools consistent responses
- Provide students with cyber-safety education designed to complement and support ICT User Agreement initiatives
- Welcome enquiries at any time from parents/caregivers/legal guardians or students about cyber-safety or any school ICT systems.
- Ensure that all ICT User Agreements are returned.

4.5 Responding to Breeches of the Cyber Safety Policy

4.5.1 Classroom Teacher or Leader identifies the Breech in the Cyber Safety Policy

- Report the breech to the relevant House leader of the student accused, and the IT team where appropriate to access any required information linked to the breech.
- Ask the student/s to complete an Incident Report Form to give their view of the incident, along with any witnesses and evidence as required and pass to the relevant House Leader.

4.5.2 House Leader Follow Up

- House leader to liaise with the IT team as required to gain all information relevant to the incident
- House leader to speak with students involved and collect any other evidence as required, including further Incident Report Forms
- House leader to follow consistent responses for the element of the breech of the Cyber Safety Policy
- House leader to contact parents/caregivers regarding the breech, and consequences for the student. This may include an SDP for the student.
- If the breech is against the law, the leader will work with Deputy Principal or Principal to contact SAPOL for further investigation.
- Leader to record incident on Daymap and notify relevant teachers as required.

4.5.3 IT Team Follow Up

- Along with collecting and providing evidence required for the investigation, the IT team will make any changes necessary to systems, processes and monitoring if the breech may put the safety of others at risk.
- Restrict the access for offending students to ICT at Seaford Secondary College as required

4.5.4 Principal or Deputy Principal Follow Up

- Support the contact of SAPOL for any breeches to the policy that are unlawful.
- Support the suspending/pending exclusion process where appropriate in line with the school consistent responses

5. IMPORTANT INFORMATION FOR STUDENTS AND FAMILIES

5.1 What is Cyber-Bullying

Cyberbullying is bullying behaviour, using digital technology, including the internet, email or mobile phones. It differs from face-to-face bullying in that the bully can 'follow' their victim 24/7, and continue the bullying in the home. Cyberbullies may take advantage of the perception of anonymity but in many cases it is clear who is behind the bullying. Cyberbullying can be particularly harmful as it is often a public form of humiliation and many others are able to see what is written or posted. Once something is published online, it is difficult, if not impossible, to remove all traces of it.

Forms of Cyber-Bullying

- sending nasty texts, picture messages, emails, or instant messages (e.g. Facebook)
- repeated prank phone calls
- using a person's screen name to pretend to be them (setting up a fake account)
- using a person's password to access their account and then pretending to be them
- forwarding others' private emails, messages, pictures or videos without permission
- posting mean or nasty comments or pictures on chat or forums
- sending and/or forwarding sexually explicit images ('sexting')
- intentionally excluding others from an online group

5.2 Important information for parents/caregivers

5.2.1 Signs that your child is being cyber bullied

- **Change in mood, demeanour and/or behaviour**: for example being upset, angry, teary or rebellious when they were not previously.
- **Change in friendship groups:** it can be normal to change friends many times during school days. Teachers can often provide insight, as they see class dynamics in action every day.
- **Spending more time with family instead of friends:** adolescence is generally a time where friends become very important and parents less so.
- **Lowering of grades**: often students who are being bullied show a distinct change in application to studies and a lowering of grades.
- **Not wanting to go to places:** a dramatic change in enthusiasm for going to school or sport—this can manifest as non-specific ailments (headaches, stomach-aches, generally 'feeling sick').
- **Being extra secretive in online activities**: being online in a 'secluded' part of the house.
- **Distinct change in online behaviours**: being 'jumpy' when text messages arrive, not leaving their phone alone, wanting to be online all the time, or never wanting to be online.

5.2.2 What to do if your child is being cyber bullied

- **Praise them for coming to you**. This is a big step as many young people may be frightened to tell a parent about cyberbullying. Even if you don't really understand, let them know that you will help them.
- **Do not be angry with your child.** Remember that they are the victim and it is someone else who is doing the wrong thing. Do not threaten to take technology away from them because of what someone else has done.
- **Do not respond to the bullying.** It is important not to respond to nasty emails, chats, SMS or comments. This is usually what the bully wants, so ignore them. It is natural in many cases to want to 'fight back', but responding with a threat may get your child into trouble as well.
- **Inform the school.** It is important that the school knows what is going on so they can provide support and monitor any issues that may spill onto the yard or classroom. If the bully is a student from the same school, the school will work through the situation as they would with any other bullying behaviours reported to them.

- **Save and store the content.** Keep copies of emails, chat logs, text messages, comments or posts. Take a screen shot of the evidence—ask your child for help to do this if necessary. An easy, non-technical way to get hard copies is to bring the content up on the screen of a mobile phone and use a photocopier to take a copy of the screen.

- **Help your child to block and delete the bully from all contact lists.** Most social networking sites allow the user to control who has access to communicate with them. Many people feel 'mean' blocking another person, even if that person has already been mean to them—you may want to sit and support your child as they do this.

- **Use the 'report abuse' button.** Most social networking sites have a method to let the site administrators know that a particular user is behaving unacceptably. Depending on the rules of the site, users can be warned or banned.

- **Have some 'down time' without technology**. It is important for both mental and physical health that your child's life is balanced so they are not constantly 'online' and spending hours on a mobile phone. This should not be used as punishment, rather as some peaceful time where they are not being bothered.

- **Get new online accounts and/or a new phone number.** There are programs that can be added to a mobile phone which will allow parents to set restrictions on the phone's use. Check with your mobile phone provider. Technology at the moment does not allow for individual numbers to be blocked in the same way that online applications do. Phone numbers can be changed at no cost, if the request for a new number is as a result of ongoing abuse.

- **If ongoing, report to police.** Most cyberbullying between students can be resolved at school level, but schools may not be able to report cyberbullying between individual students to the police so it can be up to the parent to make a police report. ACORN (Australian Cybercrime Online Reporting Network) is a service set up by the police to report cybercrimes at www.acorn.gov.au.

5.2.3 What to do if your child being a bully

It often comes as a shock to be told that your child has been bullying another student online. It is important that parents support the school in their handling of the situation. Don't try and play it down. Parents have the ability to prevent the vast majority of online bullying. Be involved, and aware of what your child is doing online. Once you are aware that your child has bullied someone else online, you can help them understand that their behaviour is both unacceptable and possibly criminal as well.

As a parent you could:

- discuss why it is not acceptable to be nasty or mean online and offline
- let them see there are consequences—don't bail them out
- acknowledge that they may be feeling guilty or awful about their behaviour, and discuss ways they can rectify the situation
- work together to improve the situation by offering an apology to the victim
- talk to them about their actions and try and find out why they behaved in this way
- ask them to imagine they were the victim—how would they feel
- develop a home-based Acceptable Use Agreement—set clear rules and boundaries about their online behaviour and your expectations and consequences for breeching this agreement
- enlist the help of your school welfare staff, GP, a counsellor or adolescent psychologist

5.3 Important Information for Students

5.3.1 What to do if you are being bullied

- **Do not respond to the bullying:** It is important not to respond to nasty emails, chats, SMS or comments. This is usually what the bully wants, so ignore them. It is natural in many cases to want to 'fight back', but responding with a threat may get you into trouble as well.
- **Save the evidence of bullying**: including screen shots, text messages etc so that you can show a teacher or parent what is happening.
- **Tell someone you trust:** Sometimes your friends aren't the best people to seek help from, as they may not have enough knowledge. Ask older siblings or trusted adults to help and support you.
- **Report the bullying to your parents and/or the school**: Remember that you deserve to feel safe and to make your own choices. Report the bullying to a teacher at school to follow the harassment and bullying process to help keep you safe and prevent further bullying from happening.
- **Block and delete the bully from all contact lists:** Most social networking sites allow the user to control who has access to communicate with them. Many people feel 'mean' blocking another person, even if that person has already been mean to them, but it is important that you are safe when using technology.
- **Use the 'report abuse' button:** Most social networking sites have a method to let the site administrators know that a particular user is behaving unacceptably.
- **Have some 'down time' without technology:** It is important for both mental and physical health that your life is balanced—so they are not constantly 'online' or spending hours on a mobile phone.
- **If ongoing, report to police:** Most cyberbullying between students can be resolved at school level, but schools may not be able to report cyberbullying between individual students to the police so it can be up to the parent to make a police report. ACORN (Australian Cybercrime Online Reporting Network) is a service set up by the police to report cybercrimes at www.acorn.gov.au.

5.3.2 Impact of Bystanders; What to do if you see bullying towards others

Sometimes it's tempting to think that if you aren't the person doing something wrong, you don't have a role to play in setting things right. If you know someone is deliberately causing problems for somebody else, you should do what you can to stop it—sometimes just a small action can prevent things getting worse.

By knowing about it and not saying anything you are allowing it to happen because bullies thrive on other people's silence and you would want someone else to speak up for you if you were being bullied. Most people who bully online also bully offline: what might seem harmless can have a negative impact on people's emotional and physical wellbeing, friendships and other relationships. When more people take positive action it creates a culture where bullying (online or offline) is not acceptable and encourages people to look for attention in more positive ways.

If you know someone is causing problems, tell them why they should stop. If you don't feel safe to say something yourself, tell someone who can take action. Even if the person being treated badly isn't your friend, they don't deserve to be the victim of things like gossip, name calling, false information, homophobia etc. You have the power to short-circuit behaviour that you think is unfair so refuse to be part of the harassment, and tell people why.

You may not be the one who has initiated some sort of campaign about another person, but even forwarding information you receive to others makes you part of the problem. It is important to stop and think about how your actions will impact on others before you engage in potentially dangerous behaviours.

5.3.3 Think about the impact of your actions on others

The online world is a part of the real world and what you do in one affects the other. When communicating with people using digital technology it is important to take the time to think about how your actions might effect another person, and how you would be effected if it was happening to you. Please remember the following:

- Try to put some 'think time' between your thoughts and actions. When we are angry and/or hurt we can feel very intense emotions. These may not be the way we feel when some time has passed. If we 'speak' too quickly we may regret what we have said.
- Seeking 'revenge' almost always escalates a situation rather than resolving it. Seek support to resolve differences with people, or ignore them to prevent the situation getting worse.
- If you are angry with a friend or in a disagreement with them, it's a good idea to speak with them about the matter that has upset you. This shows that you value the friendship and is more likely to resolve the issue than saying nasty things to other people on social media or face to face.
- Stop and think about what possible outcomes your actions might have. You might change your mind once you think through the possible consequences.
- Our physical appearance is part of our self-image and most of us want to look the best we can. Posting any images of other people, whether they have been manipulated or not, without their permission is disrespectful, and not a 'friendly' thing to do.
- The images you post become instantly available to whoever can access your page. Material that has been shared on a private basis, between friends, should never appear in the public realm.
- Before you post something ask yourself if the people that you love and respect would think that what you're putting up is ok.
- Ask yourself how you would feel if nasty comments or images of you were being posted on social media sites. Respect the privacy of others and don't post embarrassing images.
- Receiving anonymous messages that are unpleasant or threatening can be frightening and produce a great deal of anxiety for the recipient. If such messages are received repeatedly a person's mental health can be damaged.
- Using someone else's mobile phone to send malicious messages is dishonest and betrays trust. If a friend is willing to share the use of their mobile phone with you, respect their generosity and use the device responsibly.
- Because your mobile phone number is a part of your identity, you need to know what it's being used for if you allow someone else access. The number will always be traced back to you!
- Making other people the target of your pranks is often not funny for them. If it is deliberate and ongoing, or other people join in, it is bullying. What you think is amusing and 'fun', doesn't always look like that to another position. Try to walk in the other person's shoes to gain an insight into how they might experience your 'fun'.
- We all have many parts of our personality. Think about how you would feel if you were being treated as one dimensional. Don't reduce an individual to just one aspect of who they are, one decision or one action.

6. MONITORING, EVALUATION & REVIEW

This policy will be subject to review every year by the Leadership Team in consultation with relevant stakeholders, to comply with any change to school policy or priorities, applicable legislation, government or departmental policy.