Seaford Secondary College

DIGITAL LEARNING PROGRAM

Centre for Innovation

1-1 Program · Benefits to Learning
Changing World of Work · 21st Century Skills
Acceptable use of technology

Seaford Secondary College's Digital Learning Program was developed in consultation with staff, students and the community and ratified by Governing Council. The Digital Learning Program is 1-1, which means as a whole school community we commit to 1 laptop for every 1 student.

2019 Seaford Secondary College Digital Learning Program
Policy Document (last edited 01.04.2019)

1 Introduction

Today, technology has the power to transform lives. It can allow students to access information, people, and ideas that were unthought-of only a decade ago. Seaford Secondary College's Digital Learning Program was developed in consultation with staff, students, and the community and ratified by Governing Council during 2016, for 2017 implementation. The goals of the program are to:

- Ensure we have a sustainable way of achieving a 1:1 ratio of students with laptops now that the previous government funded, Digital Education Revolution, 1:1 program is complete.
- Allow students to develop essential 21st Century skills for preferred futures
- Increase student engagement in learning
- Improve student learning outcomes

The Digital Learning Program is 1:1, which means as a whole school community we commit to 1 laptop for every 1 student. Seaford Secondary College will continue to provide the necessary digital infrastructure and specialist computer rooms, utilising specialist software.

The purpose of this document is to:

- Describe the importance of digital learning in schools in the 21st Century
- Give an introduction to teaching and learning at Seaford Secondary College
- Explain the expectations of students bringing a digital learning device to school
- Provide essential information for safety, care, warranty, damage and insurance of devices
- Support students to be safe and responsible when using technology, and to be positive digital citizens
- Explain acceptable use of technology at Seaford Secondary College
- Provide an ICT User Agreement to be signed by students and caregivers before using any personal or school owned technology at Seaford Secondary College.

2 Learning at Seaford Secondary College

Current research indicates the world and workforce is rapidly evolving, and it highlights digital literacies are at the forefront of all future endeavours. Access to digital technologies is critical in preparing students for their rapidly evolving future, and the skills developed through daily access are fundamental to their learning and future choices.

At Seaford Secondary College, this is the key driving force behind our integration of technologies in the classroom. The core strategic objectives of our Digital Learning program are to develop vital 21st Century Skills, ensuring students leave Seaford Secondary College as confident, discerning and forward-thinking members of the community, both locally and globally.

Our Digital Learning Program, and the strategic integration of innovative technologies in the classroom, allows our staff to transform our teaching pedagogy and has the potential to engage students and enrich their learning experience to enhance achievement in ways not previously possible. Not only will it allow our staff to provide students with fast and effective feedback, but it will also allow us to effectively deliver more personalised learning for all students. Other benefits to students using technology for learning include:

1. More focused and engaged and therefore more learning
2. Prepares students for the global world through digital citizenship
3. Better prepares students for jobs of the future
4. Improves ability to retain information and concepts learned
5. More customised learning working at the student's own pace
6. Developed digital literacy skills
7. Faster feedback to learning from a variety of audiences
8. Improves student communication skills
9. Allows students to learn from experts all over the world
10. Greater supports students with learning difficulties.

At Seaford Secondary College we believe that students will be successful if we create safe conditions for learning, have high expectations from all learners, are able to instil a growth mindset to facing challenges in learning, and provide targeted intervention that allows all students to grow at their current level. We believe that these values, coupled with Seaford as a centre for innovation, will mean our students gain essential skills for preferred futures at the completion of their school life.

3 21st Century Skills for Preferred Futures

Research suggests that up to half of all current jobs are likely to be automated by machines in the next 10 years. This change to careers is as big as the Industrial Revolution and education must prepare young people for the new economies, with more than half of future jobs needing digital capabilites. This means new methods of education, with technology being a vital part of preparing our students for their futures. Skills Essential for 21st Century Learners include:

1. Collaboration in person and in online communities
2. Higher order thinking skills
3. Ability to follow a design process to create innovative solutions and products to problems
4. Ability to access and critically reflect on the huge amount of information available
5. Abilitiy to self-manage through extended and complex problems
6. Being safe and responsible digital citizens
7. Advanced problem solving skills
8. Coding as a new form of literacy.

Research has also shown that 1:1 programs build these essential 21st Century Skills: “The overwhelming evidence showed laptops have facilitated the development of 21st Century Skills e.g digital literacy, creativity and innovation skills, critical thinking and problem solving skills, communication and collaboration and self-directed learning amongst students.” Argueta, 2011.

4 General Policy

4.1 Student Owned 1:1

The Seaford Secondary College Digital Learning Program gives families ownership of the device, its care, insurance and warranty. 2 in 1 touch screen devices have been recommended at varying prices to support choice and varying financial capabilities.

4.2 School Network Use

Students will have access to the Seaford Secondary College DLP Network which will allow them access to a home drive, printing and internet access. There are restrictions in place to ensure students are using the school network in safe and appropriate ways. Students are reminded avoiding these restrictions is a form of hacking and leads to school suspension and police intervention. More on each of these services can be found later in this document.

4.3 Charging computers

The school prefers for students to charge their devices at home and have their laptop charged to full capacity when they leave for school, in order to get through the whole day with the benefits of digital learning. If the student requires charging their laptop at school then the following must apply;

1. Parent/caregiver has signed the content form to allow the school to tag and test the device
2. The device needs to be tagged and tested by the school with the school approved sticker in date
3. Seek approval from teacher in charge and have the teacher inspect the device
4. Understand that if the device charger is deemed unsafe/damaged to charge at school then the charger will be retained by the teacher and parents informed immediately that this device can no longer be used at school.
5. Understand that all charging at school is at the risk of the owner, including accidental damage caused whilst charging in the classroom and that the school takes no responsibility for damage occurred.
6. Understand that teachers have the right to refuse permission for students to charge their device in the classroom and that they are not to argue this point with the teacher

4.4 Backing up data at home and school

It is the responsibility of the students to ensure their data is regularly backed up. This is vital to ensure students do not lose valuable evidence of their learning. It is recommended that students save all work to their computer Home Drive as well as to an external hard drive or USB that is well looked after. Students will have access to a school home drive to store files from school owned devices.

5 Devices

After consultation with students, staff and parents Seaford Secondary College arrived at a decision on which devices would maximise learning, whilst also being most financially manageable for our community. Students and staff alike identified 2 in 1 devices as those with the best applications for teaching and learning. 2 in 1 devices offer touch screen capabilities, a fully functioning Windows computer, with a keyboard for typing fluency.

SSC has decided not to have a compulsory device that we ask all families to purchase to ensure that all families are able to find a device that is most appropriate to their circumstances. Recommended minimum requirements for a device that ensures students receive the greatest benefits to their education include:

- An 8 hour battery life to last the school day
- A 10 inch screen
- Minimum of 128 gigabyte of Hard Drive space
- Minimum 4 giabytes of RAM (8 gigabyte recommended)
- keyboard & trackpad highly recommended

5.1 Device Care

At Seaford Secondary College all students are provided access to a lockable locker. We strongly rcommend that students use these lockers during times where they do not need to use their digital device or when there is a likelihood that the device may be at risk of damage. E.g. during break times or during practical lessons such as Health and Physical Education. Students are advised to care for their laptops in the following ways:

- Always store your laptop in the carry case where possible
- Do not consume drinks or have your laptop near water or steam
- Do not wrap the cord too tightly around the power adapter or the cord will become damaged
- Try to avoid moving around with the laptop
- Be careful even with the laptop in a school bag or carry bag. Do not drop the bag from your shoulder or store the laptop in a bag with drinks
- Avoid storing other items in the case with the laptop such as headphones or USB sticks
- Do not place items between the screen and keyboard and close it, as they may damage the screen

- Use designated student lockers to store your device when it is not being used, or when going to subjects and activities that may cause risk to the device, such as PE classes.

5.2 Loss, theft & accidental damage

The use of technology, whether owned by Seaford Secondary College or student-owned devices, entails personal responsibility for the user. Approved use of devices by users during the instructional day is restricted to education related purposes. It is expected that users will comply with the Seaford Secondary College Student Behaviour Code and the Acceptable Use of Learning Technologies Policy. Responsibility to keep privately owned devices secure rests with the individual owner. If a device is stolen or damaged, it will be handled in the same manner as other personal property, which may include Behaviour Management responses. The Department for Education does not provide insurance for accidental loss or damage to devices brought to school for use by students.

5.3 Insurance

We encourage you to either purchace accidental damage Device Insurance, or contact your household contents insurance company and arrange for your device to be covered under your personal policy. Insurance means your device is covered for any accidedental damage and theft. As per 5.2, the Department for Education does not provide insurance for accidental loss or damage to devices brought to school for use by students. However, claims may be met under the department's public liability insurance where the loss or damage is attributatble to a negligent act or omission on the part of the school.

5.4 Warranty

Most new devices come with a warranty and extended warranty up to 4 years can be added. Please note this warranty does not cover any loss or theft. The warranty covers manufacturer's defects and normal use of the laptop. It does not cover negligence, abuse, malicious or accidental damage (e.g. cracked LCD screens, or liquid damage, are not covered under warranty).

5.5 Virus Protection

As students have ownership, and personal use, of their laptops in addition to connecting to the Internet from both home or school they need to take steps to protect the laptop from virus attacks. Students should ensure that anti-virus software is kept up-to-date on their devices and regularly check for viruses. There are various versions of anti-virus protection to purchase through stores or free online. Some examples include:
Avast: https://www.avast.com/en-au/
AVG: http://www.avg.com/au-en/homepage
Microsoft Security Essentials: https://support.microsoft.com/en-us/help/14210/security-essentials-download

6 Acceptable Use of Learning Technologies

6.1 Introduction

It is essential that students and families are clear on their rights, responsibilities and expectations of acceptable use of Seaford Secondary College technology, or when using personally owned devices at school. In the final section of this document you will find the ICT User Agreement, which needs to be read, understood and signed by students and caregivers. Students will be unable to access the school network or use their computer at school until this document is signed and returned to Seaford Secondary College.

6.2 School Responsibilities

- Support the rights of all members of the school community to engage in and promote a safe, inclusive and supportive learning environment.
- Have an Acceptable Use of Learning Technologies Policy, and corresponding Learning Technologies User Agreement.

- Educate our students to be safe and responsible users of digital technologies.
- Raise our students' awareness of issues such as online privacy, intellectual property and copyright.
- Supervise students when using digital technologies for educational purposes.
- Provide an at-school on Network filtered Internet service but acknowledge that full protection from inappropriate content can never be guaranteed.
- Respond to issues or incidents that have the potential to impact on the wellbeing and reputation of our students, staff and the school.
- Ensure the Acceptable Use of Learning Technologies Policy is followed by applying consequences for inappropriate use will be in accordance with Seaford Secondary College's Student Behaviour Management policy, which may include confiscation of device for evidence, Time Out, suspension and/or exclusion. Where a student is suspected of any unlawful activity, this will be reported to the South Australia Police.
- Provide parents/caregivers with a copy of this agreement.
- Support parents/caregivers to understand the importance of safe and responsible use of digital technologies, the potential issues that surround their use and strategies that they can implement at home to support and protect their child.
- Provide quality ICT infrastructure that supports quality digital learning.
- Use teaching and learning strategies that are inclusive of the laptop, in order to build 21st Century skills

6.3 Student Responsibilities:

- Read this Acceptable Use of Learning Technologies Policy carefully.
- Follow the cyber-safety strategies and instructions whenever using Learning Technologies on the school site or at any school related activity, regardless of its location.
- Ensure their device is taken to all lessons, with charge, unless the teacher has requested otherwise
- Ensure their behaviours and activities are in line with the learning program and teacher direction. Off-task behaviours will be subject to Behavior Management responses and can include confiscation of device.
- Ensure their device is fully functional and seeking swift resolution of any problems.
- 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. Understanding that any pornographic material, illegal movies/TV series/game downloads etc will result in suspension and/or exclusion. The South Australian Police will be notified regarding any unlawful activity.
- Take care of Learning Technologies. If students have been involved in the damage, loss or theft of Seaford Secondary College's technology or devices, or other student's devices, they will be subject to Behavior Management responses, including suspension and exclusion, and their family may have responsibility for the cost of repairs or replacement. There is never a reason to touch another student's device or another student's bag.
- Access applications and files in safe and ethical ways. Students must not disrupt the smooth running of any school ICT systems nor attempt to hack or gain unauthorised access to any system. The school's wellbeing and behaviour management processes extend outside of school hours or off site.
- Keep this document somewhere safe for future reference.
- Ask the relevant staff member when unsure about anything to do with this agreement.
- Report issues of concerns related to security or behaviour, including well-being, to a relevant staff member or responsible adult.
- Seek support where their own welfare or device has been affected by others, or where they become aware that the welfare or device of a peer, has been affected by others.

6.4 Cyber Safety

Staff, students and parents/caregivers must familiarise themselves with the content of the 2009 document *Cyber-safety: keeping children safe in a connected world: Guidelines for schools and preschools* (available at www.decs.sa.gov.au/speced2/pages/cybersafety).

The following is an excerpt from the overview of the Cyber-Safety document:

"Learning is a social activity. It happens when people interact with other people and their ideas, knowledge and perspectives. ICTs provide children and students with new and engaging ways to learn. ICTs expand social and knowledge networks so that children and students access current information, interact with experts and participate in peer teaching and learning.
Using ICTs they can publish their learning, as evidence of achievement or to invite feedback for improvement. It is important to both protect and teach children, students and adults, while they learn to use ICTs and become responsible digital citizens. This includes adults thinking ahead of new risks and children and students learn how to avoid exposure to inappropriate material or activities, and protecting themselves when they are online. They need to learn how to use ICTs, including mobile technologies and social networking sites, in responsible and ethical ways. In addition, they need to feel confident about alerting the adults in their lives when they are feeling unsafe, threatened, bullied or exposed to inappropriate events. In response, these adults need to take appropriate actions to protect the child or young person."

Key aspects of Cyber Safety include:

- students must not give out identifying information online, use only their first name, and not share their home address, telephone number or any other personal information such as financial details (e.g. credit card), telephone numbers or images (video or photographic) of themselves or others
- students must not use their school e-mail address in non-school online communications as this e-mail address contains their personal name and school details
- students must 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
- students must not forward inappropriate material to others
- students should never respond to message or bulletin board items that are suggestive, obscene, belligerent, threatening or make them feel uncomfortable - these messages should be reported to a teacher
- students must inform their teacher immediately if they see anything on a website that is inappropriate, unpleasant or makes them uncomfortable
- parents/caregivers and teachers should actively monitor online behaviour and encourage their child/student to follow Cyber-safe strategies.

6.5 Internet usage at school

According to DECD ICT Security, Internet Access and Use, and Electronic Mail and Use policies, 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 students 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 (e.g. viruses, worms)
- accessing files, information systems, communications, devices or resources without permission
- using for personal financial gain
- using non-approved file sharing technologies (e.g. Torrenting)
- using for non-educational related streaming audio or video
- using for religious or political lobbying
- downloading or sharing non-educational material.

While Seaford Secondary College will make every reasonable effort to provide a safe and secure online learning experience for children and students, Internet filtering is not always 100 per cent effective, and it is

not possible to guarantee that children and students will not be exposed to inappropriate material. The cost to access the Internet at school is currently included in the school fees, and allows for students to make reasonable use of the Internet for the purpose of learning. Internet traffic is monitored and students making unreasonable downloads will incur an additional fee.

6.6 Internet Use at home

Internet browsing by students at home or from other non-DECD sites is permitted. Please note this will not be filtered or monitored by Seaford Secondary College, and it is the responsibility of the student and care givers to ensure that material being accessed is safe and appropriate.

Seaford Secondary College does not provide Home-Internet provision. To ensure all students have equal right to the curriculum and the ability to excel in their learning, any assessment tasks that require home internet use will be due at least 48 hours after being assigned.

6.7 Student use of Social Media

Social media (sometimes referred to as social networking) are online services and tools used for publishing, sharing, discussing and collaborating. The list of social media types is extensive with new and innovative social media apps being continuously developed. It is important to understand that social networking can occur in open and closed online communities. An open community on the web is visible to everyone worldwide. It is possible to have a closed community which restricts information and comments to a specific group of people. At Seaford Secondary College, we acknowledge that Social Networking offers potential for teaching and learning, whilst also carrying risks. Acceptable use of Social Networking tools at Seaford Secondary College then only occurs in accordance with Cyber Safety Policy (7.3), as part of a teaching and learning program, under supervision of a teacher.

6.8 Project publishing

Technology provides an abundance of opportunities for users to utilise interactive tools and sites on public websites that benefit learning, communication, and social interaction. Users may be held accountable for the use of any information posted on these sites, if it detrimentally affects the welfare of individual users or the governance, climate, or effectiveness of the school. From time to time, teachers may recommend and use public interactive sites that, to the best of their knowledge, are legitimate and safe. As the site is “public” and the teacher, school, and DECD are not in control of it, all users must use their discretion when accessing information, storing, and displaying work on the site.

6.9 Software, apps, music, & games

It is an expectation that devices owned by students and brought to school, comply with the appropriate, legal operating system and software licensing requirements, including music, movies or games, and are appropriate for use or viewing at school. Parents/ caregivers are encouraged to regularly monitor the contents of students’ devices.

“According to a recent paper by the Massachusetts Institute of Technology (MIT), games, when developed correctly and used appropriately, can engage players in learning that is specifically applicable to school curriculum—and teachers can leverage the learning in these games without disrupting the worlds of either ‘play’ or school.” (e-School News, 2009). At Seaford Secondary College teachers may, at times, incorporate games into their teaching and learning program. In these situations, playing games or listening to music during class time, in accordance with teacher direction, is permitted.

6.10 Copyright

Students must realise their responsibilities regarding intellectual property and copyright law and ethics, including acknowledging the author or source of information. To ensure compliance with copyright laws, students must only download or copy files such as music, videos or programs, with the permission of the owner of the original material. If students infringe the Copyright Act 1968, they may be personally liable under

this law. Students are also reminded of copyright and plagiarism rules and responsibilities when completing assessment pieces and researching information created by others.

6.11 Printing

Staff and students are encouraged to transmit work electronically in line with 21st Century skills. Students have access to school printers through the school network. Students will be allocated a printing balance per term, and are reminded to ensure they use this wisely, as printing restrictions and charges will apply for unnecessary or inappropriate printing.

6.12 Consistent responses for misuse of technology.

At Seaford Secondary College, we believe that the laptop is a tool for the learning process, like any other learning resource. With this in mind, student misuse of technology in the classroom will be managed in line with the school and DECD behavior management expectations. As the device is owned by the family, teachers will not confiscate laptops unless necessary for evidence, but may ask students to put their device safely away, if it is interfering with the learning process. Students are reminded that actions including misuse, cyber-bullying, hacking, or theft can lead to restrictions, suspension and police action.

7 User Identification and Passwords

The DECD ICT Security, Internet Access and Use Policy contains the following main provisions:

- To log on to a school owned device, the school network or Daymap, students must use a unique user identification (user-ID) that is protected by a secure password.
- Passwords must be kept confidential and not displayed or written down in any form.
- Passwords must not be words found in a dictionary, or based on anything somebody else could easily guess or obtain using person-related information.
- Passwords must not be included in log-on scripts or other automated log-on processes.
- Students must not disclose their personal passwords to any other person.
- Students will be accountable for any inappropriate actions (eg bullying, accessing or sending inappropriate material) undertaken by someone else using the student's personal user-ID.

7.1 Password Tips and Tricks

- Passwords should contain uppercase letters, lowercase letters and numbers.
- Use substitute numbers for letters in words. For example, "ELEPHANT" could become "3L3PHANT", "COFFEE" could become "COFF33".
- Try to think of a sentence or phrase and use the first letter of each word. For example, "my iPad is the best" could become "mip2itb".
- From here, substitute some letters for capitals, numbers or symbols. For example, "mip2itb" could become "M!p2!tB".
- Add something on the end relating to the use for the password. For example, an iTunes account password could be "M!p2!tBTun".
- This gives a really strong password with a rating of 93% (checked using "The Password Meter" http://www.passwordmeter.com/).

8 Daymap

Daymap is the school Learner Management System which has many benefits to student learning including:

- Allowing parents to be more involved in students' learning, attendance and grades
- Allowing students to see and submit assessment pieces and learning activities, check timetables and notices for the day
- Enabling various forms of communication including messaging and the viewing of the digital school calendar

9 Training and Development

9.1 Students

It is important that students have key skills and abilities to use their laptop for the greatest learning outcomes. Seaford Secondary School staff will ensure students receive support in the following areas:

- Students will be given key information for operations such as accessing the network & printing.
- Students will learn computer and technology skills throughout various subjects to support them with the use of their device for maximum learning outcomes.
- Students will be given information to access Daymap for their learning activities and submission of assignments, check grades and feedback, communicate with staff as required, and to check their timetables and lesson notes.

9.2 Parents Daymap support

Parents are additionally able to log on to the Daymap Learning Management system to get all the benefits mentioned in the 'Daymap' section of this document to ensure everyone has the ability use the functions to support their child's learning. Parents can login to the DayMap Parent Portal via the link on the school website. To create a user parents must have a valid email address registered with the school and their child's student ID number. Assistance will be provided to assist parents in logging in, if experiencing difficulties.

9.3 Staff

On our journey of continual improvement, Seaford Secondary Staff will continue to keep up to date with technology and 21st Century teaching and learning to ensure students are using their laptops to their full potential, whilst developing essential skills for their preferred futures.

10 Acknowledgements

Seaford Secondary College would like to recognise the support from other DECD sites in writing this policy document including

- Brighton Secondary School
- Glenunga International High School
- Henley High School
- Unley High School

Seaford Secondary College will review this policy annually, to ensure it is meeting the fast-changing needs of technology in education.

11 User agreement

The remainder of this document is the ICT User Agreement which must be signed and returned to Seaford Secondary College before students are able to use any technology or access the Network at school.

ICT USER AGREEMENT

Dear Parent/Caregiver,

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), we are now asking you to read this document and sign the attached User 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 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 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 User 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 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 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, 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.

Please contact the school 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, 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. I will log on only with my own user name. I will not allow anyone else to use my account.
3. I am required to create a complex password and keep it 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 direction.
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, is 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 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 follow all Cyber-Safety practices before I put any personal information online. Personal identifying information includes any of the following:
   - my full name, address or phone number
   - my e-mail address
   - 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 this User Agreement, 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.

Parent/Caregiver/Legal Guardian Copy

To the parent/caregiver/legal guardian:

Please ensure you & your child have read the entire ICT User Agreement.
Please read this page carefully to check that you understand your responsibilities under this agreement.
Return signed User Agreement to the school.

I understand that Seaford Secondary 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 User Agreements
- respond to any breaches in an appropriate manner
- provide students with cyber-safety education designed to complement and support User Agreement initiatives
- welcome enquiries at any time from parents/caregivers/legal guardians or students about cyber-safety or any school ICT systems.

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

- reading this User 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 User 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 User Agreement I would like to discuss.

For the Student: My responsibilities include…

- reading this User 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 there is evidence that I have caused damage, loss or theft of ICT equipment/devices, I and/or my family may have responsibility for the cost of repairs or replacement
- creating a complex password and keeping it private
- 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.

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.

---

1. PLEASE ENSURE YOU & YOUR CHILD SIGN & RETURN THE COMPLETED ICT AGREEMENT FORM.
   (You will find this as the last page of your enrolment form/pack or as attached)

2. PLEASE RETAIN THESE 3 PAGES FOR YOUR REFERENCE.

School Copy

To the parent/caregiver/legal guardian:

Please ensure you & your child have read the entire ICT User Agreement.
Please read this page carefully to check that you understand your responsibilities under this agreement. Return signed User Agreement to the school.

I understand that Seaford Secondary 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 User Agreements
- respond to any breaches in an appropriate manner
- provide students with cyber-safety education designed to complement and support User Agreement initiatives
- welcome enquiries at any time from parents/caregivers/legal guardians or students about cyber-safety or any school ICT systems.

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

- reading this User 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 User 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 User Agreement I would like to discuss.

For the Student: My responsibilities include…

- reading this User 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 there is evidence that I have caused damage, loss or theft of ICT equipment/devices, I and/or my family may have responsibility for the cost of repairs or replacement
- creating a complex password and keeping it private
- 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.

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 tick the following boxes to ensure you understand important elements of the students using their own device at SSC

- ○ I understand that the school does not provide warranty, insurance or repairs on student owned devices
- ○ I understand that warranty and insurance are different and that warranty does not support repair of damage
- ○ I understand that I will need to add free or purchased anti-virus software on a student owned device
- ○ I understand that software on student owned devices is purchased by families

We have read and understand this ICT User Agreement and are aware of the school's initiatives to maintain a cyber-safe learning environment.

Student..... …… Date……
(print name) (signature)

Parent/Caregiver/Guardian .... Date ……
(print name) (signature)

PLEASE RETURN TO THE FRONT OFFICE

Office Use: EDSAS entered (Permission Code IT18):