'ALIS VOLAT PROPRIIS'

SEATON HOUSE SCHOOL

E-Safety Policy

Date Reviewed: September 2020
Next Review Date: Autumn 2022
Reviewed by: Head, SLT, ICT co-ordinator

E-Safety & ICT Acceptable Use Policy

This policy applies to all children and staff at Seaton House School, including the Early Years Foundation Stage (EYFS). Please also refer to the remote learning policy for further details.

Background

The very nature of this subject means that this policy must be as dynamic as possible and in constant review. Devices, new networks and the terminology associated with technology are developing all the time.

Our policy aims to balance the desirability of fully exploiting the vast educational potential of new technologies with providing safeguards against risks and unacceptable material and activities.

This Policy considers all technological appliances used by pupils and includes: both fixed and mobile internet; technologies that may have been provided by the School (such as PCs, laptops, webcams and digital video equipment); and technologies owned by pupils, but brought onto school premises (such as kindles).

Although a pupil may be trusted by her parents with regard to private internet use, the School has a duty to safeguard them and other pupils. The School believes in being proactive rather than reactive; therefore, supervision of technologies and educating pupils are key to enabling them to value the benefits of communication and exploration, whilst ensuring they understand the potential dangers associated and as such, are protected from them. We are only too aware that it is an impossible task to prevent pupils from the pitfalls of Internet and Device usage, but we strive to continue this constant battle by a variety of means, which will be listed as part of this policy.

Aims/Targets /Rationale/ Issues

Pupils are keen to grasp the opportunities offered by new technology and their availability, portability, miniaturisation and use of sophisticated electronic devices.
However, as with any new technology, there are associated risks which include the following:

- Exposure to inappropriate material (e.g. pornography, violence, hate sites, self-harm sites)
- Grooming
- Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords
- Online/cyber bullying
- Digital footprint and online reputation
- Health and well-being - amount of time spent online (internet or gaming)
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images) or youth produced sexual imagery
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

The School does not accept responsibility for, nor is insured against theft, loss or damage to any pupils' personal property, including electronic devices.

Procedures and Practices

The School provides pupils with Internet access and access to the School's own network through connections throughout the school. There is a generic pupil login to allow pupils access to the laptops. This login restricts pupil access to certain apps/features/sites. Pupils from Nursery have individual Google Classroom logins and work can be saved on their own Google drive. Girls in Forms V & VI have chrome books which are individually allocated and password protected. There are also Ipads which all year groups have access to with a range of suitable applications. Devices are kept in locked cupboards and are only used under staff supervision or instruction. We are mindful of the popularity of e-readers and devices such as Kindles, some of which are perfectly suitable for education. As we would like girls to become avid readers we have developed a policy for FV &VI girls to bring in their Kindles if they so wish. There is a permission slip that parents have to sign in order for girls to use their Kindles.

Rules and Regulations

The rules and regulations below are not meant to act as an exhaustive list of "dos and don'ts"; rather offer a level of consistency and guidance across each area of the school.

- Pupils may only use their assigned login
- No pupils may use ICT resources unless supervised appropriately
- The use of games is banned unless they have an educational purpose as deemed by the School
- Chat Rooms and social networking sites are not permitted
- Gambling and e-Commerce are not permitted
- Downloading or sharing of files such as music files is not permitted unless instructed by staff as part of a school project or assignment.
- The use of inappropriate images/websites/video clips is not permitted
- The use of personal camcorders, digital cameras, iPads, MP3 Players and games consoles are not permitted. Kindles are permitted in FV & VI. Mobile phones can be brought in by pupils walking to and from school but are kept in the office during the school day.
- Sending or taking data out of School is not permitted unless restricted to use of Google classroom.
- All pupils and staff must log into their own accounts every time they use a laptop or chromebooks and should log out before shutting any device down.

Measures in place to support the policy: Form I-VI

1. Induction

All pupils joining the School are inducted in appropriate use of the school's ICT facilities and other aspects of this policy by either their Form Tutor or the ICT Co-ordinator.

2. Paperwork

The ICT Agreement protects all parties by clearly stating what is acceptable and what is not. Pupils in Form I & II discuss this agreement with their Form Tutor and sign and a copy is kept on their pupil file. In Forms III-VI pupils sign the agreement after discussion with the Form Tutor or ICT co-ordinator. For reference a copy of this agreement is printed in the girls' homework planners.

3. Education
All pupils joining the school receive computing lessons. A key component of these lessons is to achieve a great understanding of the important issues of e-safety contained within this policy. We not only look at what is acceptable/unacceptable behaviour, but we also discuss the consequences of these actions. Material is age-appropriate and most of the content is based on the CEOP recommendations.

4. Whole Staff
An appropriate and relevant form of staff training takes place regularly. This will often take the format of an outside specialist talking to staff or staff taking an on-line course in e-safety (Educare). It is not the responsibility of specific members of staff to be vigilant for any instances of concern. It is the responsibility of the ***whole*** staff, whether that be on a school coach, day trips out, residential trips, break times, in lessons, or after school. We regularly remind staff of the need for this duty. Staff who are remote teaching should follow protocols advised to ensure the safety of themselves and the pupils. Staff should continue to be vigilant as in school even when teaching remotely and encourage pupils to only access appropriate material online. All remote teaching lessons where staff and/or pupils are working from home should be recorded. Professional conduct is paramount at all times whether working on site or remotely.

5. Parents
The school is keen to educate parents/guardians and regular information is sent out to them via parentmail. Additionally, parents will be invited into School to attend e-safety education/information from a specialist in the field. This is a crucial link to helping keeping children safe, since many issues that are highlighted have occurred outside of school lesson time. Whilst COVID restrictions have prevented parents attending information evenings on site an alternative video presentation has been devised and sent to all parents along with updates on relevant topics and possible areas of concern that have been highlighted either through discussions with pupils, staff or during safeguarding updates from Sutton.

6. Other
Assemblies, PSHE lessons and form groups all address cyber-bullying, safe use of the Internet and appropriate use of technologies.

Monitoring and Sanctions

The school will exercise its right to monitor the use of computer systems, including the monitoring of internet use, interception of e-mails and the deletion of inappropriate materials at all times. In circumstances where the school believes unauthorised use of the computer system is, or may be taking place, or the system is, or may be, being used for unlawful purposes, the school reserves the right to inform appropriate authorities and provide documentary evidence.

Pupils should be aware that computer/mobile phone memory, e-mails and other forms of electronic information storage and communication (including any external storage media which pupils bring into the School) may be scrutinised for the purposes of safeguarding or promoting a child's welfare. This would normally be authorised by the Head, Deputy Head or ICT Co-ordinator.

Although all staff and pupils at Seaton House School are expected to use ICT responsibly and receive specific education to define and encourage responsible use, the school recognises that it has a responsibility to counter any attempts at irresponsible behaviour which may still arise. Thus, the school's computing system is monitored and managed in a number of ways designed to inhibit abuses, specifically:

- Code of Conduct: All users agree to abide by the code of conduct and other published rules as laid out in computing lessons and in their classes or for Forms III-VI in their homework planner.
- User Logons and Passwords – all users will have assigned logons and password. Users are encouraged to keep these private.
- Access rights to confidential data – the computing staff work hard to ensure that all users understand that confidential data must be stored in folders controlled by appropriate access rights.
- Web Filtering – the School subscribes to a reputable service (RM) that maintains an on-line database that categorises websites. Some categories are banned permanently.
- Mail Filtering – keyword filtering prevents some inappropriate email leaving the school or arriving into user mailboxes.
- Computer Logs – all user logon and logoff activity is logged. All website requests are logged and users are taught this. Cygnet are our service providers who keep the logs.
- Social Networking sites – access to these is blocked onsite.
- Staff should ensure that all communication with pupils is done on agreed platforms and never on personal accounts.

Expectations of Pupils and Parents beyond the School

When a pupil is at home, families bear responsibility for the guidance of their children. The school expects the use of ICT by its pupils, even when at home, to comply with the school's stated ethos, and honour the agreement they sign permitting their use of ICT at the School. Material downloaded in the home, posted in cyber-space from a home computer, or transmitted to a mobile phone when a pupil is at home, can impact significantly upon the life of pupils at School. Thus the school requires the parents/guardians of pupils enrolled at Seaton House to cooperate with the school in the education of their children in the use of ICT.

- Most initial offences will be dealt with by Form Tutor (ensuring the Deputy Head/Head are made aware) and the removal of computer or internet usage may be a first punishment. In such circumstances parents/guardians will be notified.
- More serious offences or repeated abuse of ICT by a pupil will be dealt with by the Deputy Head or Head. In such circumstances the Deputy Head will normally write to a pupil's parents/guardians.
- Under circumstances when abuses of ICT constitute illegal activity the Head will interview the pupil with her parents (or guardians). Sanctions applied will be proportionate to the offence committed. This may also involve informing the police.

Pupil input

Pupils can voice their own views on the School's ICT provision through the School Forum (Council). They may also speak to the ICT Co-ordinator directly or via their Form Tutor.

Responsibility

If a pupil comes across inappropriate or illegal material, they must tell a teacher immediately (see ICT Acceptable Use Policy below). All pupils are also asked to inform staff or parents if they come across content or material that upsets them or makes them feel uncomfortable. The teacher should then tell the Deputy Head. Reports about suspicious behaviour towards children and young people in an online environment will be made to the Child Exploitation and Online Protection Centre (CEOP) www.ceop.police.uk. Law enforcement agencies and the service providers may need to take urgent steps to locate the child and/or remove the content. Online safety is the responsibility of the E-Safety officer in conjunction with the Designated Safeguarding Lead.

Reminders:

NEVER forward content (email, photo, website address etc.) to someone else containing *inappropriate* content.

NEVER forward content (email, photo, website address etc.) to someone else containing *illegal* content; *this is an offence*.

This policy is written by the Head in conjunction with the SLT and after consultation with relevant staff.

Links with other policies and documents

- ICT Acceptable Usage Policy – combined with this policy – see below
- School rules as laid out in the homework diary (Forms III-VI) and/or displayed in classes
- Anti-Bullying Policy
- Child Protection and Safeguarding Policy
- Remote Learning Policy

REVIEW

This policy will be reviewed every two years.

Reviewed September 2020 (updated early in response to huge change in IT provision as a result of COVID).

Judith Evans
Chair of Governors

Ruth Darvill
Headteacher

SEATON HOUSE SCHOOL

ICT AGREEMENT

Please read and tick each column to confirm you agree.	✓
1. I will not use a computer at school without a teacher present in the room.	
2. I will respect the school's ICT resources and do nothing to disable or cause any damage to them.	
3. I will ask permission before entering any website, downloading programs, apps or files from the Internet, unless my teacher has already approved it.	
4. I will not look at or delete other people's files without the teacher's permission.	
5. Any electronic communication I send will be polite and responsible. If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately.	
6. I will not access my personal email, social networking or Internet chat from a school device unless special permission is given by a teacher.	
7. I will not use any ICT equipment, either in or out of school, to deliberately hurt, upset, bully or harass anyone outside the school community.	

If I break the rules, I understand that appropriate sanctions will be applied.

Pupil's Name: ……. Pupil's Signature: ……

Form Teacher's Signature: …….

Date: …….

ICT – General Rules to be discussed with Pupils each year

Useage of Laptops, Chromebooks & Ipads in class

- No food or drink is to be taken into or consumed whilst electronic devices are in the room.
- Hands must be clean.
- Keyboards, mice, mouse mats, monitors, cables and chairs must be left tidy.
- Computers are primarily for work therefore noise levels must be kept to a minimum.

COVID – AFTER USE, ALL COMPUTER EQUIPMENT INCLUDING HEADPHONES AND MICE MUST BE DISINFECTED OR WIPED DOWN.

Printers

Good practice must be exercised when printing.

- Only print work that has been approved by a member of staff.
- Only print when absolutely necessary.
- Make sure your name is on the work you are printing out.
- Avoid wasting paper and only print in colour if truly necessary.
- Only press print once. Do not keep pressing 'print' if nothing happens.
- Remember to collect your printouts from the printer.

Logging on

- You must never attempt to alter system settings and software.
- You must not attempt to install software on the system.
- You must log off when leaving a computer to prevent someone else using your login.
- All computers should be logged out and all programs closed before shutting down.

Internet and E-mail

You must always behave in a responsible way, paying particular attention to the following:

- Never attempt to look for unsuitable/rude/illegal pictures or information. If you find anything like this by accident, close down those pages **immediately**. Remember that the pages you visit, and for how long, are logged. **Tell a teacher or adult what you have found**.
- Do not "download" unnecessary material. It can contain viruses and pictures can take up a lot of disk space on the server.
- 'Chat rooms' and social networking sites, such as Bebo and Facebook are **not** to be used – they should be blocked by the school's RM filter.
- The playing of games is **not** permitted unless of an educational nature and with staff permission.
- Do not reveal personal details such as your name, age, address and telephone number to anyone online.

Interactive Whiteboards

- You must only touch or use them with staff permission.
- You must not use any type of ink pens on an interactive whiteboard.
- You must not stick anything to, poke or scratch an interactive whiteboard.

Mobile Devices

- This includes mobile phones, laptops (see below), iPods, iPads, e –readers, voice recorders and other devices that have the ability to record or show images, sounds or video.
- You must have written permission from the Head Teacher before you bring a mobile phone or other electronic device into school, and provide a good reason why you need to do so.
- Kindles and e-readers are allowed in Forms V & VI but a permission slip is required.
- You must switch off any device you bring in while on school premises unless authorized by a member of staff.
- You must leave any mobile phone or device, which is not solely an e-reader, that you bring into school with the School Office or unless authorized by a member of staff.
- You must not take a device on a school trip.

General

Irrespective of whether electronic devices are used or not, girls are expected to show consideration for others at all times. All pupils will be held accountable for their own actions.

SEATON HOUSE SCHOOL

FURTHER INTERNET SAFETY ADVICE FOR PARENTS

All our pupils are taught at some stage how to research on the internet and to evaluate sources. Not only does this technological revolution give young people unrivalled opportunities, it also brings risk. This booklet is designed to give parents more information about what we do in school to help keep children safe, and to provide parents with some practical advice about how they can support our efforts in this area at home.

WHAT WE DO IN SCHOOL:

- It is an important part of our role at Seaton House to teach our pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, cyber-bullying, harassment, grooming, stalking and abuse.
- Children's use of the internet at school is always supervised, and all computers have an appropriate filter. Using the internet safely is often discussed during lessons through the school.
- Our Designated Safeguarding Leads have received appropriate training in the safety issues involved with the misuse of the internet and other mobile electronic devices. We seek to work closely with parents in promoting a culture of e-safety, and we will always share any concerns we may have about a child's behaviour in this area with parents.
- All pupils spend the first half of the Autumn Term doing E-Safety from Forms I – VI and pupils are encouraged to make use of various online resources that are available from specific internet safety sites (listed in the following section).
- Teachers discuss the 'Acceptable Use guidelines' with their class during the first Computing lesson of the year, using age-appropriate language and those items applicable to a particular class.

Background

The internet is a 'place' where you children mix with others and share their lives. Just as in any other area of life, if you don't know what your children are doing, where they are going or who they are mixing with, you risk compromising their safety.

Thankfully the 'grooming' of youngsters on the internet remains rare, however it is nevertheless important to be vigilant. Remember that an adult using a social networking site can become anyone they want to be when they are online.

Despite its lower profile, internet bullying occurs more frequently than grooming. Threats, harassment and psychological torment via email of in a virtual chatroom can have a devastating effect on a child. There is also a new threat of radicalisation whereby extremists are able to target children with the sole purpose of winning them over to join terrorist organisations.

Social networking sites

The main focus of this booklet is on general internet and email use, and as it is not recommended that children of primary school age have access to social networking sites, this will only be mentioned briefly. As children enter secondary school you will need to be aware of these relevant issues which will affect them as they get older. Some parents may have seen an article in the Telegraph which reported on research carried out in the Netherlands about the impact of Facebook on exam results. The research suggests that students who use Facebook while studying for exams scored on average 20 percent lower than people who did not use Facebook while working. We cannot comment on the veracity of the research but it certainly raised questions that we at school, and perhaps parents, may want to discuss with our children.

WHAT PARENTS CAN DO AT HOME:

- Firstly, you need to discuss as a family whether you feel your child is old enough to be using the internet independently. There is no 'right' or minimum legal age for this, but you need to consider whether your child is mature enough to be able to cope with any risks and if you have the time to provide the necessary supervision. There is, however, a minimum age for subscribing to certain social networking sites.
- Discuss with your child any rules for internet use, for example you might want to restrict use beyond school work to 1 hour per day, or weekends only, or before a certain time at night. As parents you need to be in control and ensure that they adhere to any rules agreed upon.
- Ensure you have an appropriate filter installed on your home computer (e.g. Optenet or Net Nanny. Norton also have this as an add-on to their normal anti-virus software). This parental control software will allow you to block access to certain types of websites, to restrict use at certain times or to log your child's internet activity. It can also prevent email traffic from undesirable sources.

- It is not recommended for children under the age of 10 to have their own email address. However when they do get one, keep the following in mind particularly during the initial period: Consider asking them to give you their password so you could potentially check any messages (you will need to explain that this is not to invade their privacy, but merely to protect them while they are still 'new' users); ask them to tell you if an unknown person sends them an email so you can delete it an block their address; tell them not to forward 'chain' emails to their friends as this may give others access to their address book; tell them not to divulge ANY personal information in an email or on their profile; don't let them use a webcam with people they don't know personally.
- Your home computer should preferably be in an area of the house where you can frequently visit (e.g. a family room or living room/kitchen area) rather than in bedrooms.
- Learn as much as possible about what your child does online. Ask them to show you the sites they have visited and to tell you who they have exchanged messages with. They may not reveal everything but it's a good start – at least they will know you are interested.
- Check the history of sites your child has visited, and be explicit that you will do this regularly. If the history has been deleted, ask them why.
- Talk to other parents about the rules they have for their children and share good ideas.
- Children of primary school age should not be posting pictures of themselves on social networking sites – there is plenty of time for this in secondary school. Parents need to decide at what age they would feel comfortable with this. However, you also need to remember that you do not have control over what your children's friends post on the internet and that they may well be included in group photos.
- Be aware of how, when and where your child uses the internet. This will help you to spot any significant changes, for example if they spend much longer online than usual, or they start using the internet only away from home. This may well be nothing more than typical adolescent behaviour, but at least you will be alert to other possibilities.
- If possible, block pop ups on all internet sites as these are unnecessary distractions and might have inappropriate content.
- Look out for changes that may signal your child is being bullied or harassed. These can include loss of confidence, withdrawal from family life, anxiety or argumentativeness, insomnia or lack of concentration.
- Visit some of the following internet sites which have useful resources for both parents and children: www.thinkuknow.co.uk ; www.childnet-int.org ; www.cyberbullying.org ; www.cybermentors.org.uk ; www.digizen.org.uk; https://www.nspcc.org.uk/keeping-children-safe/online-safety/; https://nationalonlinesafety.com/

KEEP SMART, KEEP SAFE!

Encourage your child to follow the 5 SMART rules when using the internet and mobile phones:

S SAFE:

Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M MEET:

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' permission and even then only when they can be present.

A ACCEPTING:

Accepting emails, instant messages or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE:

Information you find on the internet may not be true, or someone online may be lying about who they are. Make sure you check information before you believe it.

T TELL:

Tell your parent or another trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.