Online Safety Policy

This policy also applies to the EYFS

Updated	Review Date	Version
September 2022	September 2023	2022.01

Signed: Mr John Clarke (Chairman of the Board)

Online Safety Policy

In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and email. Computer skills are vital to access life-long learning and employment; indeed, computing is now seen as an essential life-skill.

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which, as in life generally, may be unsuitable. It is important that schools, libraries and youth clubs, as well as parents, adopt strategies for the safe and responsible use of the Internet.

This Policy should be read alongside the following policies

- Anti-Bullying
- Policy on Taking, Storing and Using Images of Children
- PSHE Scheme of Work
- RSE
- Safeguarding and Child Protection

Abercorn School Online Safety Policy

Why Abercorn School has an Online Safety Policy

The Internet is an open communications channel, available to all. Applications such as the Web, email and chat all transmit information over the wires and fibres of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be more restricted elsewhere. Sadly, email and chat communication can provide opportunities for adults to make contact with children for inappropriate reasons. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

Schools need to protect themselves from possible legal challenge. The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly an offence to hold images of child pornography on computers and to use Internet communication to 'groom' children. However, the possession of other obscene or offensive materials is not clearly covered. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Schools can help protect themselves by making it clear to users that the use of school equipment to view or transmit inappropriate material is "unauthorised". However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable and appropriate steps have been taken to protect pupils.

Teachers will be aware of many risks of Internet use but may not have had opportunities for detailed discussion. Advice and training from advisers or child protection officers should be sought. Policy writing should involve discussion and a policy agreed by staff will be easier to implement than one imposed.

Our Focus

Supervision is the key strategy. Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation. Is it sufficient for a teacher or learning support assistant to be in the area? Should Internet machines be placed in a common area between classrooms? Are there circumstances outside normal lesson time where pupils justifiably need access to the Internet?

Aimless surfing should never be allowed. It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "Why are we using the Internet?"

Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. Of course the experienced teacher will choose a topic with care, select the search engine and then discuss with pupil's sensible search words, which should be tested beforehand. A fruitful group or class investigation may result – contrast this with possible individual frustration.

Pupils do not need a thousand websites on weather. A small selection may be quite enough choice for juniors. Favourites are a useful way to present this choice to pupils. If teachers' website selections for various topics are put on the each classes Google Classroom page, access by pupils from home and by other schools is made possible.

There may even be difficulties here. One recommended site, successfully used by primary schools, suddenly changed into a pornographic site. Presumably hackers had infiltrated the site or taken over the domain. Sites should always be previewed.

Government advice on email has been revised. The concern is the possibility of access to pupils by adults of unknown intention, if email is not controlled. Students are provided with @abercornschool.com email addresses. Students are not able to email a person outside of the domain. The email system is fully managed and all ingoing and outgoing emails are regularly monitored.

In brief:

- *Discuss with pupils the Responsible Computer and Internet Use, Rules for Pupils.*
- *Regularly monitor all incoming and outgoing email.*
- *Preview all sites before use and consider off-line viewing.*
- ***Plan the curriculum context for Internet use to match pupils' ability.*** *Vigilance is essential and supervision the most important strategy.*

Core Principals of Internet Safety

The Internet is becoming as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated Internet access brings with it the possibility of placing of pupils in embarrassing, inappropriate and even dangerous situations. Schools need a policy to help to ensure responsible use and the safety of pupils.

The Abercorn School Online Safety Policy is built on the following five core principles:

Guided educational use
Significant educational benefits should result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

Risk assessment
21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time, they must learn to recognise and avoid these risks – to become 'Internet Wise'. Schools need to ensure that they are fully aware of the risks and implement a policy for Internet use. Pupils need to know how to cope if they come across inappropriate material.

Responsibility
Internet safety depends on staff, schools, directors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as phones. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

Regulation
The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied, for instance unmoderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions.

Appropriate strategies
This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies must be selected to suit the school situation and their effectiveness monitored. There

are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

Abercorn School Online Safety Policy

Who will write and review the policy?
Our Online Safety Policy has been written by the Computing staff using government guidance. It has been discussed and reviewed by the Senior Leadership Team. It will be reviewed annually, or as required.

Why is Internet use important?
Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet access is an entitlement for students who show a responsible and mature approach to its use.

Internet access is an essential tool for today's online learning environment. It is likely that children will be using the Internet and engaging with social media far more during this time. Our staff are aware of the signs of online bullying and other online risks and our filtering and monitoring software remains in use during this time to safeguard and support children. Our staff will follow the process for online safety set out in our Child Protection Policy and Procedure. Staff and students should not form online relationships, especially on social media.

How does the Internet benefit education?
Benefits of using the Internet in education include:

- Access to world-wide educational resources.
- Inclusion in government initiatives such as the DfES Computing in Schools;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LEA and DfES;
- Mentoring of pupils and provide peer support for them and teachers.

How will Internet use enhance learning?

- The school Internet access will be designed expressly for pupil and staff use and will include filtering appropriate to the age of users.
- Pupils and staff will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed annually to reflect the curriculum requirements and age of users.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils and staff will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

There are also IT and online security implications of any online learning environment, with consideration given to who is able to access what. All staff have received full training and guidance in this area, and the School has asked for parental permission for children to access our Remote Education which extends into remote homework now that all children are expected back at school. We have also taken measures to ensure that any content is suitable for the age of the children accessing it.

How will pupils learn to evaluate Internet content?

- If staff or pupils discover unsuitable sites, details of the site content and web link must be reported to the IT Department, who will inform our filtering provider to update their filtering settings.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Training should be available to staff in the evaluation of web materials and methods of developing students' critical attitudes.

How will email be managed?

- All pupils will be set up with an email account that can only email staff and students from Abercorn School.
- Pupils must immediately tell a teacher if they receive an offensive email.

- Pupils must not reveal details of themselves or others in email communication, such as address or telephone number, or arrange to meet anyone.
- Excessive social email use can interfere with learning and may be restricted.
- The forwarding of chain letters is not permitted.

How should Website content be managed?

- The point of contact on the Website should be the school address, school email and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully.
- Pupils' full names will not be associated with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website and the FOA website.
- The Head will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

What are newsgroups and email lists?

Newsgroups will not be made available to pupils.

Can Chat be made safe?

Pupils will only be permitted to use internal communication services such, as Gmail and Google Meets, using their allocated school email account.

Sharing of sexual images

Although Abercorn School does not allow pupils to bring mobile phones into school until Year 7, it is always possible that a pupil may bring a device into school without permission, therefore staff and pupils should be aware of the consequences of sharing nudes or semi-nudes. Year 7 and above mobiles are handed in and stored in the office until the end of the day. The sharing of nudes or semi-nudes can be defined as images or videos generated by children under the age of 18 or of children under the age of 18 that are of a sexual nature or are indecent. These are also referred to as Youth Produced Sexual Images or nudes of semi-nudes. It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence.

How can emerging Internet applications be managed?

Emerging technologies will be examined for educational benefit before use in school is allowed.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. None of Abercorn's mobile devices have access to a 3G/4G/5G network, therefore anyone accessing such a network will usually do so on their own personal device which the School can't control or manage.

Adults may bring mobile phones to the school premises, but must not use them in the presence of children, unless in an emergency and never to take pictures of children.

How will Internet access be authorised?

Upon joining Abercorn School the admissions office will issue a Welcome pack which will consist of an Internet Access agreement.
From entry, pupils will be granted access to our schools email facility and may use these facilities when a unit on online safety and email communications has been completed.

Access to online resources will be granted from entry, upon completion of the signed Welcome pack, which will grant consent for their child or children to use of the Internet and online resources at Abercorn School.

How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

The use of computer systems without permission or for inappropriate purposes will result in disciplinary action and Internet access denied.

Methods to identify, assess and minimise risks will be reviewed annually.

The Head of Computing and the Head will ensure that the Online Safety policy is implemented and compliance with the policy monitored.

How will filtering be managed?

The IT team will continually monitor, test and review the web filtering and safeguarding software we use. Filtering strategies will be selected by the school after relevant research and trials of available options. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil. The IT manager and technician will regularly check the logs within the filtering software and report any potential concerns to the relevant staff member or DSL. If there is a high level concern, such as extremism, an email will be sent directly to the IT manager who will review the incident and complete a Record of Concern form and send it to the DSL.

If staff or pupils discover unsuitable sites, details of the site content and web link must be reported to the IT Department, who will inform our filtering provider to update their filtering settings. Filtering is provided by the following:

- Cisco Meraki
- Senso.Cloud
- Sophos

The School is aware of its responsibilities regarding the Prevent Duty and will endeavour to ensure that children are safe from terrorist and extremist material when accessing the Internet through the school systems and will establish appropriate levels of filtering. The IT team will ensure that filtering is in place on all school devices and that any illegal or inappropriate sites are blocked. Filtering will be applied at all times on student Chromebooks that are taken home as personal school devices. We block all websites suggested by the Home Office.

To prevent students being drawn into terrorism we actively monitor for selected keywords that are typed into devices. If a keyword is detected, this will be logged by the filtering software and where possible, a screenshot will be taken. The website will be blocked.

Any material that the school believes is illegal will be added to the school's blacklist immediately by the ICT department and will be referred to the content filter providers.

How will the policy be introduced to pupils?

- The Acceptable Use Policy will be posted in all rooms where the Internet is available. These rules will be developed through the School Council and from examples from other schools.
- A copy of Acceptable Use Policy will be given to parents when they are asked to consent to Internet use.
- Pupils will be informed that Internet use will be monitored. They will be informed that online bullying is a serious matter and that their accounts will be monitored if we suspect

it is happening. If there is any evidence of this, their accounts will be immediately suspended.
- Instruction in responsible and safe use should precede Internet access. This will take place in computing lessons.

How will staff be consulted?

- All staff must accept the terms of the Staff Handbook and Staff ICT Acceptable Usage statements before using any Internet resource in school.
- All staff including teachers, classroom assistants and support staff, will be provided online with the School Online Safety Policy, and its importance explained at the first staff meeting of each year by the Head of Department.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by the Computing department.
- Staff development in safe and responsible Internet use, and on the school Online Safety policy, will be provided as required.
- Staff have the opportunity to express their opinion about Internet use at staff meetings or directly to HOD.
- Staff should refer to guidelines within the Staff Handbook.
- New staff members should contact the ICT Manager at the commencement of their employment for their training on this policy and consent form completion.

How will Computing system security be maintained?

Local Area Network security issues include:

- The user must act reasonably. Loading non-approved software could cause major problems. Good password practice is required including logout after use.
- The workstation should be secure from casual mistakes by the user.
- Cabling should be secure and wireless LANs safe from interception.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured to a high level.
- Virus protection for the whole network must be installed and current.

Wide Area Network (WAN) security issues include:

- All external connections must be assessed for security risks including any wide area network connections or VPN's.

- Firewalls and routers should be configured to prevent unauthorised use of software such as FTP and Telnet at the protocol level.

Decisions on security made by external agencies such as the LEA or ISP must be discussed with the school. Third-party security testing should be considered.

The Internet is a connection to the outside world that could compromise system performance or threaten user or system security. The downloading of large files such as video and MP3 can compromise system performance. A wide area network (WAN) connection introduces further risks such as pupils trying to access another school. However, it also brings the opportunity for industrial strength security in the form of hardware firewalls and the expertise to design and operate them.

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated daily.
- Microsoft Windows and Office updates will be installed and updated daily, as required.
- The content filters will perform a daily update of the blacklist.
- Security strategies will be discussed by computing staff.
- Use of portable media such as floppy disks, memory sticks and CD-ROMs will be reviewed. Portable media may be brought into school and be virus checked using a computer that is connected to the internet.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.

How will concerns regarding Internet use be handled?

Responsibility for handling incidents will be delegated to the Deputy Heads respectively

Any complaint about staff misuse must be referred to the SLT who will investigate.

Pupils and parents will be informed of the complaints procedure which involves speaking with the HOD in the first instance.

Parents and pupils will need to work in partnership with staff to resolve issues.

As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Sanctions available include:

- Interview/counselling by Head of school;
- Informing parents or carers;
- Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Website.
- Current pupils should have received a copy of the 'Responsible Computer & Internet Use Rules for Pupils' and signed, along with their parents, a consent form which will be valid throughout the pupil's time at Abercorn School.
- New pupils will be required to read the 'Responsible Computer & Internet Use Rules for Pupils' and asked to sign an online agreement prior to using online services at Abercorn School Internet access will be granted. The consent form will be valid for the pupil's time at Abercorn.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet can be made available to parents.
- Childnet will be invited to the school once every two years, to talk with the parents about Internet Safety.

Appendix A
Notes on the legal framework

The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Computer & Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice)

(Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day to day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Schools could start by banning private use of a school's computer system, but then allow private use following application to the Head. The Rules for Responsible Computer & Internet Use, which every user must agree to, contain a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring.

The following legislation is also relevant:

General Data Protection Regulation 2016/679 concerns data on individual people held on computer files and its use and protection.

Copyright, Design and Patents Act 1988 makes it an offence to use unlicensed software.

The Telecommunications Act 1984 Section 43 makes it an offence to send offensive or indecent materials over the public telecommunications system.

Protection of Children Act 1978

Obscene Publications Act 1959 and 1964 defines 'obscene' and related offences

Appendix B
Student - ICT Acceptable Usage Policy

These rules help us to be fair to others and to keep everyone safe.

I will ask permission before using the Internet.

I will use only my own account and password, which is secret. I will not give this information to anyone else.

I will only look at or delete my own files.

I understand that I must not install software on any computers owned by the school.

If I bring files into school on a USB stick, I must show my teacher and have their permission before I use them.

I will only email people I know and who my teacher has approved.

The messages I send will be polite and sensible.

I am aware that online bullying is a serious matter and I will not be using ICT as a tool to hurt my fellow pupils.

I understand that I must never give out my home address or phone number, or arrange to meet someone I do not know.

I will ask permission before opening an email or an attachment sent to me by someone I do not know.

If I see anything I am unhappy with or I receive messages I do not like, I will tell the teacher immediately.

I understand the school may check my files, emails or websites I have been on if they wish.

Food and drink is not allowed near computing equipment at any time.

I will be responsible for the files uploaded onto my Google drive ensuring that I log out after use.

I understand that if I break these rules I may not be allowed to use computers or the Internet.

The school may exercise its right to monitor the use of the school's computer systems; including access to files, websites, school email account and deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or storing unauthorised or unlawful text, imagery or sound.

Appendix C
Letter to Parents

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of computing skills, Abercorn School is providing supervised access to the Internet and online services. We believe that the effective use of technology and online tools are an essential skill for children as they grow up in the modern technological world. Please would you read the attached Rules for Responsible Computer and Internet Use. From Nursery, children will receive their email account which will allow access to their online Google classrooms.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. We have a comprehensive Online Safety policy in place. You can view this policy through the school website. The Abercorn School Computing department operates filtering systems, including Senso.Cloud, which restrict access to inappropriate materials. We can provide references to information on safe internet access at home if you wish.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, Abercorn School cannot be held responsible for the nature or content of materials accessed through the Internet. Abercorn School will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Abercorn School Internet use (or to see a lesson in operation) please telephone me to arrange an appointment.

Yours sincerely,

The Senior Leadership Team

Appendix D

Consent Form

Abercorn School

Responsible Internet Use

Please complete, sign and return to your form teacher

Pupil's name:

Form:

Pupil's signature:

Date:

Pupil's Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the Computer system and internet in a responsible way and obey these rules at all times.

Parent's Consent for Internet Access

I have read and understood the school Rules for Responsible Internet Use and give permission for my child to access the internet. I understand that Abercorn School cannot be held responsible for the nature or content of materials accessed through the internet. I agree that Abercorn School is not liable for any damages arising from use of the internet facilities.

Date:

Parent's signature:

Please print name:

Appendix E
Chromebook Loan Agreement (currently Years 5 - 9)

Dear Parents and Carers,

As part of our 1:1 Chromebook programme the pupils are issued with their own Chromebook for the duration of the time they are at Abercorn School.

Pupils will be given the laptops at the start of Year 5, or whenever they join Year 5, and they must be returned upon leaving at the end of the summer term in Year 9, or before if the pupil leaves the school. We expect the laptops to be returned in the same condition and that pupils treat them with respect and care. The standard school responsible computer and internet use agreement still applies to these computers and pupils should not download anything without express permission from the school.

Due to the value of the Chromebooks, we ask that you please sign and confirm that you will be responsible for the first £300 of the excess if there is any loss or damage whilst the laptop is assigned to your child. You are very welcome to put this on your household insurance if you wish. Unfortunately, without your signature the laptops cannot be removed from school and pupils cannot therefore use them for remote learning or during their time at Abercorn.

Please could you sign and return this letter confirming your agreement.

Pupil's name: _____

Items loaned:

Chromebook

Chromebook charger

Laptop bag

Signed: _____

Print name: _____