Strathearn School
E-Safety Policy

Approved by Board of Governors –

Signed :________________________________

(Chair of Governors)

Review Date	Amendments
May 2022	
May 2025	

1. Introduction

1.1 Rationale
Digital Technology has become an integral part of the lives of pupils in today's society. Digital Technology and the online world have opened up a range of opportunities for pupils and have the potential to add value to pupils's education. However, alongside this, there is a growing concern about the negative impact that these technologies could potentially have if not used safely.
As a school we need to be progressive about our response to the ever-increasing reliance on Digital Technology and the changes it brings to our society.

At Strathearn we believe that there are significant benefits that come from learning, exploring and connecting with each other online. We also know how important it is to make sure pupils know how to protect themselves. Strathearn is committed to raising awareness of the potential risks pupils face online and how these concerns can be reported. The School will ensure each pupil is educated about how to act appropriately online and stay safe.

The potential risks pupils may encounter online are grouped into 4 categories.

<u>Conduct</u>
A Pupil may be at risk because of their own behaviour, for example, by sharing too much information.
Some of the conduct risks pupils may face include:

- The potential for excessive use which may impact on the social and emotional development and learning of the pupil;
- Plagiarism and copyright infringement;
- The sharing / distribution of personal images without an individual's consent or knowledge;
- Digital footprint and online reputation;
- Sexting.

<u>Content</u>
Age-inappropriate or unreliable content can be available to pupils.
Some of the content risks pupils may face include:

- Exposure to inappropriate content, including online pornography and violence;
- Access to illegal, harmful or inappropriate images or other content;
- Lifestyle websites, for example eating disorders, self-harm or suicide sites;
- Hate sites;
- Access to unsuitable video / internet games;
- Content validation: an inability to evaluate the quality, accuracy and relevance of information on the internet.

Contact

Pupils can be contacted by bullies or people who groom or seek to abuse them.
Some of the contact risks pupils face may include:

- Inappropriate communication / contact with others, including strangers;
- The risk of being subject to grooming;
- Cyber-bullying;
- Identity theft and sharing passwords.

Commercialism

Pupils can be unaware of hidden costs and advertising in games, apps and websites.
Some of the commercial risks pupils may face include:

- Pop-ups and spam emails;
- In-app purchasing;
- Advertising.

As with all other risks, it is impossible to eliminate these risks completely. It is therefore our aim, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with them.

The School must demonstrate that it has provided the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. The E-Safety Policy that follows explains how Strathearn intends to do this, while also addressing wider educational issues, in order to help pupils be responsible users and to stay safe while using the internet and other communications technologies for educational, personal and recreational use.

1.2 Scope

For the purpose of common understanding, this policy assumes the following definition of e-safety:

"E-Safety is about using electronic devices in a safe, responsible and respectful way. It means safeguarding children and pupils in the digital world and educating them to keep themselves safe online".

NI Executive E-Safety strategy and policy for NI 2019-2022

Pupils are expected to behave online in a way that does not compromise their own safety, the safety of others or the reputation of the School. All staff and pupils are expected to adhere to this e-safety policy and this policy should be used in conjunction with our Anti-Bullying, Acceptable Use and Safeguarding & Child Protection Policies.

In relation to incidents that occur during school hours, we will work with parents, staff and pupils to ensure the e-safety of all involved, and, if necessary, to apply sanctions as per our Positive Behaviour Policy.

In relation to e-safety incidents that occur outside of school hours, the School will work with pupils and parents to help keep all pupils safe and offer educative support where appropriate. E-Safety outside school hours is primarily the responsibility of the parents. If inappropriate activity occurs outside school hours with the intention of having a negative effect on any member of the School community, and this is brought to our attention, then we will liaise with parents as to an appropriate way forward. Any issues that arise inside school, as a result of e-safety incidents outside of school, will be dealt with in accordance with school policies.

2. Roles and Responsibilities

2.1 Board of Governors

The Board of Governors have a duty to safeguard and promote the welfare of pupils and to determine the measures to be taken by the School to protect pupils from online abuse. In exercise of these duties, the Governors must ensure that an E-Safety Policy has been approved and implemented. Oversight of the operation of this policy will be through the Curriculum Committee.

The Principal

The Principal will:

- Have overall responsibility for e-safety;
- Support the Designated Teacher for e-safety in the development of an online safety culture within the School.

Vice-Principal (Pastoral)

The vice-principal (pastoral) will be the Designated Teacher for E-Safety and will:

- Act as a named point of contact on all online safety issues and liaise with other members of staff and agencies as appropriate;
- Keep up-to-date with current research, legislation and trends and adjust policy and practice accordingly;
- Coordinate participation in events to promote positive online behaviour, e.g. Safer Internet Day;
- Ensure that online safety is promoted to parents/carers and the wider community through a variety of channels and approaches;
- Maintain an online safety incident/action log to record incidents and actions taken as part of the School's safeguarding recording structures and mechanisms;
- Monitor the School's online safety incidents to identify gaps/trends and adjust policy and practice accordingly, and report to the Principal as appropriate;
- Ensure that online safety is integrated with other appropriate school policies, procedures and guidelines;
- Ensure all members of staff receive regular, up-to-date and appropriate training regarding online safety and provide guidance regarding safe, appropriate communications;
- Ensure that suitable, age-appropriate and relevant filtering is in place to protect pupils from inappropriate content to meet the needs of the School, and ensure that the filtering and School network system is actively monitored;
- Work with and support technical staff in monitoring the safety and security of the School's systems and network.

The Designated Teacher may delegate some aspects of the responsibilities listed above to members of the wider Pastoral Team (Senior Teacher (Pastoral), Heads of Year, Form Tutors), as appropriate.

E-Learning Co-ordinator

The E-Learning Co-ordinator will:

- Lead the ICT committee in promoting e-safety among pupils through the delivery of E-Safety Newsletters;
- Liaise with the Vice-principal (pastoral) to explore ways of promoting e-safety to pupils, parents and staff;
- Liaise with the Vice-principal (pastoral) to coordinate participation in events to promote positive online behaviour, e.g. Safer Internet Day;

- Keep up-to-date with current research, legislation and trends and adjust policy and practice accordingly;
- Contribute to the development of E-Safety Policies;
- Develop an effective ICT curriculum which promotes age-appropriate online safety messages for students on how to stay safe and how to take responsibility for their own and others' safety.

ICT Support Officer
The ICT Support Officer will:

- Ensure that the use of the School's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the Designated Teacher for e-safety;
- Regularly monitor the use of the network and report any breaches or concerns to the Designated Teacher for e-safety and together ensure that they are recorded, and appropriate action is taken.

Staff
Teaching and non-teaching staff will:

- Contribute to the development of E-Safety Policies and procedures;
- Adhere to the School E-Safety Policy and Acceptable Use Policies;
- Sign and return the Agreement Form appended to any relevant Acceptable Use Policy;
- Have an awareness of e-safety matters and how they relate to pupils ;
- Model good practice in using new and emerging technologies;
- Embed e-safety education in curriculum delivery where possible;
- Report any concerns to the Designated Teacher for E-Safety;
- At all times adhere to the School Code of Conduct for Staff and Volunteers.

Pupils
Pupils will:

- Contribute to the development of E-Safety Policies and procedures;
- Read the Schools E-Safety Policy and Acceptable Use Policies, and adhere to them;
- Sign and return the Agreement Form appended to any relevant Acceptable Use Policy;
- Seek help from a trusted adult if things go wrong, and offer support to others that may be experiencing online safety issues;
- Take responsibility for keeping themselves safe online;
- Take responsibility for improving their awareness and learning in relation to the opportunities and risks posed by new and emerging technologies;
- Assess their personal risk of using any particular technology, and behave safely and responsibly to limit those risks.

Parents
Parents should:

- Understand the School's E-Safety Policy, Acceptable Use Policies and encourage their daughter(s) to adhere to them;
- Sign and return the Agreement Form appended to any relevant Acceptable Use Policy;
- Read all information regarding e-safety shared with them by school;
- Support the School in their e-safety approaches, and reinforce appropriate safe online behaviour at home;
- Model safe and appropriate uses of new and emerging technology.

3. Communication of e-safety

3.1 Policy access
This policy is available, on request, from the School Reception and on the School website.

3.2 Professional development for staff
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- E-safety information will be made available to new staff as part of their induction. Where necessary training and e-safety updates will also be provided during the academic year.
- All new staff should receive e-safety information as part of their induction programme, ensuring that they fully understand the School E-Safety and Acceptable Use Policies.

3.3 Education of pupils
The education of pupils in e-safety is an integral part of the School's provision allowing pupils to recognise and avoid e-safety risks and to build their resilience. E-safety is promoted through, but not limited to:

- Specific ICT lessons;
- ICT across the curriculum;
- Talks from external agencies (e.g. PSNI);
- Personal Development lessons delivered through the LLW curriculum;
- Assembly;
- Safer Internet Day;
- Anti-bullying week;
- E-safety newsletters created by the sixth form ICT committee.

3.4 Education of parents
The School recognises that parents have an essential role to play in enabling their daughter(s) to become safe and responsible users of the internet and digital technology. Parents' attention will be drawn to the Schools E-Safety Policy and expectations. Information and guidance for parents on online safety will be made available in a variety of formats, e.g. E-safety Newsletter. Parents will be encouraged to model positive behaviour for their daughter(s) online.

Parents are strongly encouraged to have regular conversations with their daughter(s) about the benefits and dangers of the Internet, to empower them to use the Internet safely.

3.5 Managing emerging technologies
There is an ever increasing reliance on Digital Technology, and as a school, we aim to be progressive about our response to changes Digital Technology brings to our society. The School will risk-assess any new technologies before they are allowed in School, and will consider any educational benefits that they may have. The School keeps up-to-date with new technologies and will quickly develop appropriate strategies for dealing with new technological developments and any associated risks.

4. Cyber bullying

For the purpose of common understanding, this Policy assumes the following definition of cyberbullying:

"Cyber bullying, or online bullying, can be defined as the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else".

UK Safer Internet website

Staff should be aware that pupils are vulnerable to cyberbullying both in and out of school. This form of bullying is considered within the School's Anti-Bullying Policy as well as in this E-Safety Policy.

The anonymity that can come with using the Internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. However, most messages can be traced back to their creator. Although there is no specific legislation for cyberbullying, the following may cover different elements of cyberbullying behaviour:

- Protection from Harassment (NI) Order 1997 - http://www.legislation.gov.uk/nisi/1997/1180
- Malicious Communications (NI) Order 1988 - http://www.legislation.gov.uk/nisi/1988/1849
- The Communications Act 2003 - http://www.legislation.gov.uk/ukpga/2003/21

Offensive material relating to the School, or any member of the School community, should not be posted online, regardless of whether this has been done at School or in any other place.

- All instances of cyberbullying are forbidden and will be dealt with according to the School's Anti-Bullying Policy.
- If pupils think they are being bullied online, they should speak to a member of staff or a parent as soon as possible.
- If staff feel that they are abused online, they should speak to a member of SLT as soon as possible.

Mobile Phones

The School recognises that many parents may wish their daughter to have a mobile phone for use in cases of emergency. However, mobile phones can be used inappropriately and they are potential targets for theft and online bullying-type behaviour. The School reserves the right to confiscate a pupil's mobile phone and retain it at Reception until 3.30 pm, should a pupil fail to co-operate with the arrangements outlined below. Pupils will need to sign for their phones to retrieve them. Pupils who persistently fail to adhere to these arrangements will be disciplined in accordance with the School's Positive Behaviour Policy.

- The use of mobile phones is restricted to lunch time, break time, before Registration and after 3.30pm. Phones must be SWITCHED OFF AT ALL OTHER TIMES, including between classes, unless directed otherwise by staff.

The misuse of mobile phones and other personal electronic communication equipment for online bullying-type behaviour will not be tolerated (see Anti-Bullying, Positive Behaviour, Internet Acceptable Use and Social Media Policies).

5. Published content

5.1 School Website

The contact details on the website will be the School address, email and telephone number. Staff or pupils' personal information will not be published. While the Principal may delegate the day to day operation of the website, the Principal will take overall editorial responsibility for online content published by the School and will ensure that content published is accurate and appropriate. The School website will comply with the School's current policy and guidelines for publications including use of pupils' images, respect for intellectual property rights, privacy policies and copyright.

5.2 Publishing images and videos online

Use of images and video is an increasingly important element in modern educational practice. Videos can be produced by staff or pupils for a variety of educational purposes as well as for promotion and recording of activities.

Images and videos may in some circumstances be published to an external storage or video sharing website. Where this is the case, current school guidelines on the use of these facilities will be followed by pupils and staff.

The School will ensure that written permission from parents has been obtained before images/videos of pupils are electronically published.

5.3 Managing Email

The School will provide all pupils and staff with at least one official email address. These addresses are the only ones which should be used for school communication and educational purposes.

School email can be monitored by senior staff. Pupils and staff will be made aware of the appropriate use of email and the sanctions if they abuse the email system. They will also be advised to be careful regarding with whom they share this email address. Pupils will be advised that this email address should only be used for school related activities and that it is not private.

These addresses may be used to allow pupils to access services which the School has sanctioned, as appropriate, for use within school (e.g. cloud-based storage and associated applications). Use of email accounts and any services accessed using that account will only be used in accordance with the current school guidelines.

5.4 Official school Use of Social Media

Official social media used by the School will be in line with existing policies, including Anti-Bullying, Safeguarding and Child Protection. Images or videos of pupils will only be shared on official school social media sites/channels in line with the guidelines on image use which can be found in our Safeguarding and Child Protection Policy.

Social media use will be age appropriate. The School is aware that many social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within School specifically for pupils under this age.

Information about safe and responsible use of School social media channels will be communicated clearly and regularly to all members of the School community. The Principal and Designated Teacher for e-safety must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence. Parents and pupils will be informed of any official School social media use, along with expectations for safe use and School action taken to safeguard the community.

Where social media is used as part of a lesson or other educational experience this will be under the control of a member of staff. Staff discretion is advised and should be in line with the current guidelines and the Staff Code of Conduct.

Official use of social media sites by the School will only take place with clear educational or engagement objectives with specific intended outcomes e.g. revision forums or increasing parental engagement. Staff use of social media sites as communication tools will only be used with permission of the Principal. School social media channels will be set up as distinct and dedicated social media site or accounts.

School social media accounts will be sanctioned by the Designated Teacher for E-Safety and will be set-up and managed by a member of School staff.

Staff will use School provided email addresses to register for, and manage, official School approved social media channels. Members of staff running official School social media channels must ensure that they obtain prior permission from the Principal/Vice-Principals, are aware of the required behaviour and expectations of use, and will monitor the use of the channel(s) to check they are being used safely, responsibly and in accordance with local and national guidance and legislation.

All communication on official School social media platforms will be clear, transparent and open to scrutiny. Any online publication on official School social media sites will comply with legal requirements including GDPR, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information, and will not breach any common law duty of confidentiality or copyright.

Staff will not engage with any direct or private messaging with pupils or parents through Private social media accounts and should communicate via recognised School communication channels.

Any concerns regarding the online conduct of pupils, parents, or staff on social media sites should be reported to the Designated Teacher for E-safety or Designated Teacher for Child Protection and will be managed in accordance with existing School policies such as Anti-Bullying, Staff Code of Conduct, Safeguarding and Child Protection.

6. Management of systems

6.1 Data security
Personal data will be recorded, processed, transferred and made available according to General Data Protection Regulations (GDPR).

All users will be informed not to share passwords with others and not to login as another user at any time. Staff and pupils must always keep their passwords private and must not share them with others or leave it where others can find them. All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their passwords private.

6.2 Filtering
The School uses a filtered Internet and email service provided by C2K. The system is designed to filter sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.

If a member of staff or pupil should unwittingly discover an unsuitable site, the URL should be reported to the ICT Support Officer or the Designated Teacher for e-safety. This will then be recorded and escalated as appropriate to C2K.

Any deliberate access to prohibited/unsuitable sites (within School or using a School-owned device) will be dealt with, as appropriate, according to the School's policies on Pupil Positive Behaviour/Code of Conduct for Staff and Volunteers.

6.3 Applications and Software used to Record Pupil Information
The Principal is ultimately responsible for the security of any data or images held of pupils. Apps/systems which store personal data will be assessed prior to use. Only School issued or sanctioned devices will be used for apps that record and store pupils' personal details, attainment or photographs.

Devices will be appropriately protected if taken off site to prevent a data security breach in the event of loss or theft.

7. Policy Review

This policy will be reviewed every three years from the date it is approved by the Board of Governors.

8. Associated Policies

The following policies/other School documents are associated with this E-Safety Policy:

- Acceptable Use of the Internet;
- Anti-Bullying Policy;
- Positive Behaviour Policy;
- Safeguarding and Child Protection Policy;
- School Owned iPad Acceptable Use Policy for Pupils;
- School Owned iPad Acceptable Use Policy for Staff;
- Use of Personal ICT Devices Policy;
- Use of personal ICT Devices in School – Staff: Conditions and Agreement;
- Code of Conduct for Staff and Volunteers;
- Conditions for Using Images of Pupils, Consent Form.