Strathearn school

E-Safety Policy and Procedures

Version History:

Date	Amendment

Section 1: Introduction

1.1 Rationale

All schools should have their own E-Safety Policy, which must operate in conjunction with other school policies including Behaviour, Child Protection, Anti-Bullying and Acceptable Use. E-Safety must be built into the delivery of the curriculum. ICT is a compulsory cross-curricular element of the revised curriculum and schools must ensure acquisition and development by pupils of these skills.

DENI E-Safety Guidance, Circular number 2013/25

Strathearn is committed to ensuring safe and responsible use of the internet and associated technologies. The school will ensure each pupil is provided with a broad range of advice and training on how to keep safe and behave appropriately whilst online and how to report concerns. E-Safety also encompasses keeping associated technologies safe from viruses, malware and associated programs.

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.

It is the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. E-Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

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 young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

1.2 Scope

This policy applies to all members of the school community who have access to and are users of the school ICT systems, both in and out of school. In relation to incidents that occur during school hours, we will work with parents, staff and pupils to ensure E-Safety of all involved, 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.

Section 2: Key Roles and Responsibilities

2.1 The 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 at a school to protect pupils from abuse. In exercise of these duties, The Governors must ensure that the school has a policy on the safe, healthy, acceptable and effective use of the Internet and other technology tools. They must also actively promote safe and acceptable working practices for all staff and pupils. Oversight of the operation of this policy will be through the Curriculum Committee.

2.2 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;
- Constitute an E-safety Committee.

2.3 E Safety Committee

The E Safety Committee will:

- Support the Designated Teacher for E-Safety in the development of an online safety culture;
- Ensure there are appropriate and up-to-date policies, procedures and guidelines regarding online safety;
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices;
- Work with the Designated Teacher for E-Safety to review online safety incident logs and using them to inform and shape future practice.

2.4 Designated Teacher for E Safety

The Designated Teacher 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;
- Liaise with the school's ICT support to keep up to date with current ICT provision and issues ;
- Coordinate participation in events to promote positive online behaviour, e.g. Safer Internet Day;
- Ensure that online safety is promoted to parents and 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 schools 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 E-Safety Committee and/or Principal as appropriate;
- Ensuring that online safety is integrated with other appropriate school policies, procedures and guidelines;
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications;
- Ensure that suitable, age-appropriate and relevant filtering is in place to protect children 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 schools systems and networks.

2.5 ICT Support

In relation to E-Safety, ICT Support will:

- Provide a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised;
- Take responsibility for the implementation of safe security of systems and data;
- 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;
- Monitor the filtering of outside service providers (eg C2K and Classnet);
- Report any breaches or concerns to the Designated Teacher for E-Safety and together ensure that they are recorded, and appropriate action is taken as advised;

- Liaise with service providers as appropriate on technical infrastructure issues;
- Ensure that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.;
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.

2.6 Teaching and Support Staff

Teaching and support Staff will:

- Contribute to the development of e-safety policies and procedures;
- Understand the school's E-Safety Policy, Social Media, Email, Internet and Storage and Acceptable Use Policies (AUPs) and adhere to them;
- Be diligent with the security of school systems and data for which they have responsibility;
- Have an awareness of e-safety issues, and how they relate to the pupils in their care;
- Model good practice in using new and emerging technologies;
- Embed e-safety education in curriculum delivery wherever possible;
- Update software on school devices as required;
- Report any concerns to the Designated Teacher for E-Safety.

2.7 Pupils

Pupils will:

- Contribute to the development of e-safety policies;
- Read the Pupil Acceptable Use Policies and adhere to them;
- Respect the feelings and rights of others both on and offline;
- Seek help from a trusted adult if things go wrong, and support others that may be experiencing online safety issues;
- Take responsibility for keeping themselves and others 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.

2.8 Parents

Parents should:

- Understand the school's Acceptable Use Policies, encourage their children to adhere to them, and adhere to them themselves where appropriate.
- 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.

Section 3: Online Communication and safer Use of Technology

3.1 Managing the 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.

3.2 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 use of these facilities will be followed by pupils and staff.

The school will ensure that all images are used in accordance with the school image use policy. In line with the schools image policy, written permission from parents will always be obtained before images/videos of pupils are electronically published.

3.3 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 to 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 (eg 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

3.4 Appropriate and Safe classroom Use of the Internet and Personal Devices

3.4.1 Use of the Internet

All internet access provided within school is filtered by C2k or Classnet. Access to websites with inappropriate content is monitored by these providers. The school has some flexibility in this area and staff discretion is advised when requesting access to sites. While staff cannot guarantee that no inappropriate content will appear, they should, as far as is possible, check the content of any requested site before use.

Pupils should never be directed by staff to access websites which are blocked by the school's filtering. When asked to conduct any work which uses the internet, pupils should be given clear instructions as to the scope and focus of the task. While many tasks will require a degree of exploration, staff will brief pupils as to expectations in terms of what constitutes quality and relevance and how to check the veracity of the information found.

3.4.2 Use of Mobile Phones and Personal Devices

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 bullying. 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 sanctioned.

- The use of mobile phones is restricted to **lunchtime, breaktime, 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 cyberbullying will not be tolerated (see Anti-Bullying Policy, e-Safety, ICT Acceptable Use and Digital Media Policy and Sanctions).

Staff discretion is advised when asking pupils to engage in any activity which would require them to use personal devices. Pupils will be advised as to what is appropriate

and inappropriate. Pupils will be made aware of the laws concerning inappropriate use of these devices.

It is difficult for staff to monitor pupils' personal internet enabled devices. Parents will be advised of their responsibility when providing this facility for their children to access the internet through an external provider. While it is not the school's responsibility to police the content of these devices we will provide information and advice to parents to help them make informed decisions with regard to this. Use of these devices inside school is liable to the same laws as outside of school. Pupils will be made aware of the laws concerning inappropriate use of these devices.

- The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- Mobile phones and personally-owned devices must be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- In accordance with JCQ regulations, phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- Pupils should protect their phone number by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices, and will be made aware of boundaries and consequences.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and unless specifically sanctioned, only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Section 4: Social Media

4.1 General Use of Social Media

Social media may include blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others. The school recognises that social media play an important role in society and has many positive benefits.

The school discourages excessive social media use within school as this can be a distraction to classwork and study.

The school will control pupils and staff access to social media and social networking sites whilst on the school network.

4.2 Official school Use of Social Media

Official social media use by the school will be in line with existing policies including anti-bullying, child protection and safe guarding. Images or videos of children will only be shared on official school social media sites/channels in accordance with the school image use 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 children 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 at the direction of a member of staff. Staff discretion is advised and should be in line with the current guidelines.

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 for educational or engagement purposes.

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 will ensure they are aware of the required behaviour and expectations of use, and will ensure that sites are 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 the Data Protection Act 1998, 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, copyright etc.

Staff will not engage with any direct or private messaging with pupils or parents through social media and should communicate via recognized 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, Child Protection and Safeguarding.

Section 5: Education, Training and Support

An online safety (E-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.

Education about safe and responsible use will precede internet access.

All users will be informed that network and Internet use will be monitored.

Up-to-date and appropriate staff guidance will be provided for all members of staff on a regular basis.

The school recognises that parents have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology. Parents' attention will be drawn to the school online safety (E-Safety) policy and expectations. Information and guidance for parents on online safety will be made available in a variety of formats. Parents will be encouraged to role model positive behaviour for their children online.

Section 6: Management of Systems

6.1 Data Security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly.

All users will be informed not to share ID's passwords with others and not to login as another user at any time. Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it. 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 password private.

6.2 Filtering

The school uses educational filtered secure broadband connectivity through the C2K and Classnet which is appropriate to the age and requirement of our pupils. These providers use systems designed to filter sites that fall into categories such as pornography, racial

hatred, extremism, gaming, sites of an illegal nature, etc. If staff or pupils discover unsuitable sites, the URL will be reported to ICT Support or the Designated Teacher for E-Safety and will then be recorded and escalated as appropriate.

The school has some flexibility outside of this filtering as to whether to block or allow use of certain sites. Decisions about which sites should or should not be filtered will be made according to the current filtering guidelines.

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 children. 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 children's 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.