Strathearn School

E-Safety Policy

Review Date	Author
May 2022	R. Armstrong
March 2026	R. Armstrong

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' 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 School 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;
- Sharing nudes or semi-nudes (often referred to as '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 people displaying bullying-related behaviour(s) 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 School 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:

"Online safety relates to all engagement in the online world. It means supporting and empowering children and young people to engage in online activities in an educated, safe, responsible and respectful way".

An Online Safety Strategy for Northern Ireland 2020-2025

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 Addressing Bullying Type Behaviour, 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 and Pastoral 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 tasks in respect of the list above to The Head of ICT/E-Learning Coordinator, or members of the wider Pastoral Team (Senior Leaders (Pastoral), Heads of Year, Form Tutors), as appropriate.

E-Learning Co-ordinator

The E-Learning Co-ordinator will:

- 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 take responsibility for their own and others' safety.
- Collaborate with the ICT Committee to evaluate and enhance the delivery of e-safety lessons within ICT classes.
- Support the ICT committee in developing assemblies for Safer Internet Week to promote positive online behaviour.
- Support parents by providing details on the Jamf Parent Ap, and other means of supporting E-safety at home.

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 School's 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;
- Encourage open conversations about online experiences;
- Model safe and appropriate uses of new and emerging technology.

3. E-Safety education and Communication

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.
- Teacher Professional Learning around e-safety will be provided as/when appropriate through the annual TPL programme.

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;

Pupils will be guided on how to download and use the Safer Schools NI app as part of their e-safety education.

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 School's E-Safety Policy and expectations. Information and guidance for parents on online safety will be made available in a variety of formats, e.g. monthly E-safety Newsletter shared via ParentMail. 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.

The School encourages all parents to download and use the Safer Schools NI app, which provides up-to-date information, guidance and resources to support online safety at home.

We also recommend the use of Jamf Parent as a tool to monitor and restrict pupils' access on School issued iPads at home. As the School can only manage these devices during the school day, Jamf Parent provides parents with additional control and oversight outside of school hours.

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.

3.6 Artificial Intelligence

Although the Department for Education (DfE) guidance applies primarily to schools in England, we acknowledge its relevance in shaping safe and effective use of Artificial Intelligence (AI) in education. Strathearn School will continue to monitor developments in AI guidance and adapt its practices to ensure pupils and staff engage with AI tools responsibly, ethically and in line with safeguarding principles.

3.7 Digital Wellbeing

We recognise the importance of promoting digital wellbeing alongside e- safety. Digital wellbeing will be embedded in Personal Development lessons, assemblies and pastoral support. We will encourage balance between online and offline activities, and support pupils in managing the impact of digital tools on their wellbeing.

4. Cyberbullying

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

"Cyberbullying, 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 Addressing Bullying Type Behaviour 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 Addressing Bullying Type Behaviour Policy.
- If pupils think they are experiencing bullying-related behaviour 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 Addressing Bullying Type Behaviour Policy and Positive Behaviour Policy). ~~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. This permission is sought when new pupils are inducted into the School.

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 (supported by the ICT Support Officer). 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 Addressing Bullying Type Behaviour, 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. celebrating pupil success, 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 Addressing Bullying Type Behaviour, 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 where they can be found. 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. Digital Wellbeing

Strathearn School recognizes the importance of promoting digital wellbeing alongside E- safety. Digital wellbeing will be embedded in Personal Development lessons, assemblies and pastoral support. We will encourage balance between online and offline activities, and support pupils in managing the impact of digital tools on their wellbeing.

8. Policy Review

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

9. Appendices and Associated Policies

The following documents are appended to this E-Safety Policy and form part of its implementation framework:

Appendices

- **Appendix I** – School-Owned iPad: Acceptable Use Policy for Pupils
- **Appendix II** – School-Owned iPad & EA Portable Device: Acceptable Use Policy for Staff
- **Appendix III** – Use of Personal ICT Devices Policy for Pupils: Conditions and Agreement

Associated School Policies

These Policies are referenced throughout the E-Safety Policy and should be read in conjunction with it:

- Acceptable Use of the Internet
- Addressing Bullying Type Behaviour Policy
- Positive Behaviour Policy
- Safeguarding and Child Protection Policy
- Code of Conduct for Staff and Volunteers
- Conditions for Using Images of Pupils – Consent Form
- Controlled Assessment Policy and Procedures

Also:

- JCQ Guidance on Malpractice:
    - The JCQ AI Use in Assessments
    - Plagiarism in Assessments

Appendix I

Strathearn School

School Owned iPad: Pupil Acceptable Use Policy (AUP) and Procedures

Review Date	Author

May 2022	L. Turner
Oct 2025	L. Turner

School Owned iPad - Introduction

Strathearn School is committed to innovating with educational technology to enhance teaching and learning and communication within our School community. We embrace the opportunities which iPad technology offers us and permit the use of an authorised Apple iPad in a manner consistent with the established teaching and learning objectives of the School. We also recognise and encourage the use of the iPad for educational purposes at home.

This policy applies to all student users of Strathearn iPad hardware and software applications. It applies to all iPads used by our students, wherever they are physically located - within the School, used in a Partner School or at home. It is intended to complement the School's wider Policy on E-Safety and all other relevant School policies. Due to the nature of information and communications technology the policy will undergo periodic review and as such the School reserves the right to amend any sections or wording at any time.

Section A – Overview of School Owned iPad

The School retains ownership of all iPads, cases, accessories and apps. iPads are provided to students on a loan basis and at all times remain the sole property of the School. The School will provide all required components to ensure the iPad operates effectively in the classroom and, should it decide to offer Wi-Fi access, maintains the right selectively to filter internet content and manage the use and connection of devices to the School network in line with its E-Safety Policy.

Section B – Use of the iPad

i. Taking Care of iPads

Students are responsible for the general care of the iPad, case and power accessories. iPads or cases that are broken or fail to work properly should be reported as soon as possible to the ICT Support Officer. The School may provide replacements or a repaired iPad at its own discretion. Before any repair or replacement a parent / guardian will be required to sign and return the appropriate paperwork provided by the School - see Appendix 1.

Power accessories and cases are not covered by the School, however replacement power cables can be purchased from the School Stationery Store run by the Finance Department. Damaged cases should be reported as soon as possible to the ICT Support Officer. Faulty Apple chargers should be replaced with another Apple charger of a suitable specification for charging the device. iPad chargers are larger than iPhone chargers and only proper Apple iPad chargers should be used with the School iPads at home.

ii. General Precautions

- iPads must never be left in any unsupervised area unless in a bag or locker.
- If left in School overnight the iPad must be left locked in the student's locker.
- iPads must not be put inside heavy school bags or bags with items that may damage the iPad.
- Students should take care of school bags with iPads in them.

iii. Carrying iPads

- The School supplied protective case must be used with the iPad at all times.
- Power chargers should be left at home as the iPad should hold a charge for the duration of lessons.
- Avoid placing too much pressure or weight on the iPad screen with books or folders especially if stored in full or heavy school bags. Consider taking a book out and carrying it to relieve the pressure.

iv. Using iPad at School (General)

- iPads are intended for use at School each day. In addition to teacher expectations for iPad use, School messages, announcements, planners, calendars and schedules may be accessed using the iPad. Therefore, students are responsible for bringing their iPad, fully charged, to all classes each day.
- If students leave their iPad at home, they are responsible for completing any assignments or coursework as if they had their iPad present. Spare iPads will not be available to students who forget to bring their iPad to School or who fail to charge their iPad.
- At all times, the class teacher's decision is final regarding use of iPads, collectively or individually.
- Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
- Only apps provided by School in the Self Service app and School profiles may be placed on the iPad. School profiles are applied by the mobile device management system.

v. Using iPad at School (Photographs / Images, video and audio)

- Photographs may only be taken on the iPad when authorised by a member of staff in relation to school work. The iPad cameras are not to be used at any other time to save space and misuse of the iPad.
- Photographs / images, video, audio stored on the iPad will be deleted after they are needed, except for important school work or coursework required files which should be backed up to cloud storage.
- In accordance with this and the School's Acceptable Use of the Internet Policy, the School reserves the right to randomly check any iPad for unsuitable content.
- No images, audio or video recordings taken with a School iPad may be uploaded from any device to social networking sites by students. If required these can be shared with staff for promotional purposes.
- Recording of Strathearn staff or other pupils is prohibited unless specifically permitted by the class teacher and/or the member of staff to be photographed, audio or video recorded.

vi. Charging the iPad Battery

- iPads must be brought to School each day in a **fully charged** condition. Students need to charge their iPads each evening. It may take up to 3 hours to fully charge the iPad.
- Only authorised Apple iPad chargers suitable for the provided iPad must be used.
- iPads can be turned off or put into airplane mode when they are not required to save battery power during the School day.
- Students are not permitted to use the power sockets in School to charge any device.

vii. Accounts, Passwords and Apple IDs

- iPads work with a School Managed Apple ID, specific to its allocated user. These Apple IDs are managed by the School. Apple IDs are used to backup iPad settings so, if a replacement is required, the settings are applied to the replacement iPad.
- All account details should be kept secure by the owner. Students are prohibited from sharing this password with anyone else except their parents or as requested by senior teaching staff.
- Students may not attempt to access other student or staff accounts or iPads at any time.
- Group work files can be shared via cloud storage so the group can work if others are out of School.

viii. Home Use

- Students are allowed to use their iPads outside of School with Parent / Guardian consent. The iPad can connect to other wireless networks to assist them with homework, coursework etc. It is the responsibility of the Parent / Guardian to monitor and oversee iPad use outside of School i.e. within the home setting.
- Photographs may only be taken on the iPad when authorised by a member of staff in relation to School homework. The iPad cameras are not to be used at any other time to save space and prevent misuse of the iPad.
- It is advised that digital devices such as School iPads be charged overnight away from bedrooms.

ix. Managing files and saving work

- It is the student's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. iPad malfunctions are not an acceptable excuse for not submitting work. Therefore, students should back up all work to cloud storage such as OneDrive or Google Drive as provided to schools by C2K.
- Students can also access files and folders on the School C2K networked drives via My School -> My Files.
- All C2K provided storage areas have space to allow for School work to be saved for as long as students are in post primary education; so there is no need for files or emails to be deleted. However, folders and files should be organised by school year and subject, with meaningful filenames used. This advice also includes the C2K cloud storage, OneDrive and Google Drive.

x. Software and Apps

- The School's mobile device management system audits the iPads daily gathering data on installed apps, web clips, profiles that are on the iPads.
- Periodic checks will be made to ensure the iPads are being kept up to date and are in a useable state.

xi. Software Updates

- The operating system will show that updates are available from time to time with a red dot on the Settings icon. Students are expected to allow iOS updates a few days after they become available and should update at home when the iPad is charging.
- Upgrade versions of apps are available from time to time. Students will be expected to allow these updates when they are available.
- If there is a difficulty with update to iOS or apps, make sure there is enough free space on the device to allow them to install. Apps can be removed and added again via Self Service. Documents, videos and photos can be uploaded to cloud storage and then removed from the device.

xii. Procedure for reloading software

- If technical difficulties occur or illegal apps or networking profiles (e.g. non School approved) are discovered, the iPad will be reset. The School does not accept responsibility for the loss of any software or documents deleted due to a re-format and re-image.
- Resetting iPads is a last resort measure carried out only if necessary when other solutions fail.

xiii. Inspection

- Students may be selected at random to provide their iPad for inspection to ensure they comply with the E-Safety Policy and the Acceptable Use of the Internet Policy.
- If a PIN or password is required to access the iPad, students must share this information or face disciplinary action deemed appropriate in keeping with the School's Positive Behaviour Policy.

Section C - Acceptable Use Section

In addition to the School's Policy on the Acceptable Use of the Internet and the E-Safety Policy, the School permits use of an Apple iPad in a manner that supports the School's aims and objectives and is in line with all School policies.

This policy is provided to make all users aware of their responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the user terms and conditions named in this policy, privileges may be terminated, access to the School's network may be denied, and the appropriate disciplinary action shall be applied in line with the School's policies on the Acceptable Use of the Internet and the Positive Behavioural Policy.

i. Parent / Guardian Responsibilities

Parents are expected to talk to their children about the values and standards that they should follow on the use of the Internet and online services, just as they do on the use of all media information sources such as television, books, movies, radio, telephones, advertisements etc.

Parents and students should familiarise themselves with the details in Section B in case of accidents, theft or misuse.

ii. (ii) Student responsibilities:

- Use an iPad in a responsible and ethical manner;
- Obey general School rules concerning behaviour and communication that apply to all digital devices and their use;
- Use all School digital resources in an appropriate manner;
- Turn off and secure their iPad after they are finished working to protect their work and information;
- Report any app or system containing inappropriate content or questionable material;
- Report any email containing inappropriate or abusive language, or if the subject matter is questionable;
- Report any damage to the iPad as soon as possible to the ICT Support Officer.

iii. Return of iPad

- There is a return of iPad form available from the School Office to help prepare for returning the equipment should a pupil leave the School early – see Appendix 2.
- As part of a planned recall of iPads the device should be returned to the School undamaged, when requested, in the supplied case, with an appropriate working Apple charger plug power adapter.
- iPads in their School case, with an appropriate authentic Apple iPad charger, will be returned to the School Office if a student leaves the School early.
- When returning an iPad, it must have a completed and signed return form to confirm everything has been returned, that outstanding items have been paid for and to note if there are any faults or issues.

iv. Prohibited Activities

In addition to the guidance outlined in the School's wider policy on Acceptable Use of the Internet, students are **not** permitted to:

- Use or take another student's iPad;
- Use a staff member's iPad without consent;
- Use others' usernames or passwords;
- Trespass in others' accounts including email, folders or files;
- Take any photographs, video or audio recordings other than those directed by a member of staff;
- Upload any such photo, audio or video content to any social networking sites;
- Use the School's Apple TVs without a staff member's consent or when unsupervised;
- Intentionally waste limited resources;
- Stream video or audio, e.g. live radio, when not part of a taught lesson;
- Album picture share with others;
- Airdrop to others without prior consent;
- Download illegal content or material which is inappropriate;
- Attempt to 'Jailbreak' their iPad [modify the iPad to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorised software];
- Send or display offensive messages or material;
- Install or transmit copyright materials;
- Use obscene language or content;
- Damage devices, peripherals, computer systems or computer networks;
- Change iPad settings (exceptions include personal settings such as font size, brightness, etc);
- Attempt to modify, upgrade or self-repair devices issued by Strathearn School;
- Get repairs done independently. Any issues found must be reported to the School.
- Use a mobile phone to hotspot your iPad, in order to bypass C2K restrictions when in School.

v. Legal Propriety

- Students should comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If a student is unsure, they should ask a teacher or parent / guardian.
- Use or possession of hacking software is strictly prohibited and violators will be subject to sanctions. Violation of the law may result in criminal prosecution or disciplinary measures.

vi. iPad Identification

Student iPads will be labelled in the manner specified by the School. iPads can be identified in the following ways:

- A sticker label with the student's name on the back of the iPad case is advised;
- The device name in Settings -> General -> About should match the student's username;
- The device Serial Number.

vii. Disciplinary measures

Any student who persistently refuses to co-operate or violates any aspect of this Policy ~~or the Acceptable Use of the Internet Policy~~ may face disciplinary action deemed appropriate in keeping with the School's Positive Behaviour Policy.

viii. Staff Action

A student will be required to hand over their iPad to a member of staff if:

- the iPad is not being taken care of appropriately;
- there is a suspicion that the iPad has unsuitable material stored on it;
- a student has disrupted a lesson through improper use of an iPad;
- a student has misused her iPad to take photographs, video or audio recording on the School premises for which she has not received permission;
- the iPad or any of its features has been used for any form of bullying;
- games are being played on the iPad during class time without permission;
- the iPad is being used to stream video or audio outside of a class lesson at teacher direction;
- the iPad has been used to breach any School rule or Policy.

ix. Student and Parent / Guardian Agreement Form

Please complete the form and return it to the Form Tutor. By signing the Student and Parental/Guardian Consent Form you are agreeing to abide by the School Owned iPad Pupil Acceptable Use Policy and Procedures, the E-Safety Policy and the Acceptable Use of the Internet Policy. This agreement lasts for the entire enrolment at Strathearn School.

There is a small fee to cover the iPad Air's insurance for the School year. Please note that this does not cover the Apple charger, power cable or case. If the charger is damaged or broken you will be required to replace it with an official Apple replacement. When the student receives the iPad you should check over the items received to note the condition they are in and to confirm that they are functioning. Should the School provided iPad case start to come apart or be damaged it should be reported to the School so it can be replaced or a suitable replacement can be sought.

The fee of £35 per year will be invoiced by the School Finance Office and is to cover insurance for the iPads. This covers any fees required to repair or replace loaned iPads in the first instance. After the first repair or replacement, parents are responsible to pay the full amount of repair or replacement for any further iPad mishaps within the time an iPad is allocated.

This Policy may be updated/amended. New versions of this Policy may be found on the School website or a hard copy will be available through the School Office.

Outside of the scheduled review of this Policy, parents will be informed of changes via Parent mail.

School Owned iPad Agreement Form

Please complete and return to Form Tutor. The fee of £35 per year will be invoiced by the School Finance Department and is to cover insurance for the iPads. This covers any fees required to repair or replace loaned iPads in the first instance. After the first repair or replacement, parents are responsible to pay the full amount of repair or replacement for any further iPad mishaps within the time an iPad is allocated.

Student Section:

I accept and will adhere to the guidelines and conditions outlined in the School Owned iPad: Pupil Acceptable Use Policy (AUP) and Procedures

Student name: _____
(please print clearly)

Form Class: _____

Student Signature: _____

Date: _____

Parent / Guardian Section:

I have read and agree to the conditions outlined in the School Owned iPad: Pupil Acceptable Use Policy (AUP) and Procedures

Parent / Guardian name: _____
(please print clearly)

Parent / Guardian Signature: _____

Relationship to student: _____

Date: _____

Appendix 1

Date:

Dear Parent / Guardian,

It has come to our attention that your daughter has damaged her School iPad.

We have taken the decision to issue her with a replacement iPad as not having one is likely to impact her ability to participate fully in learning. However, this is on the condition that, should she damage another School iPad within the current academic year, you will be liable for the full cost of its repair or replacement.

I would ask that you sign and return the slip below to indicate that you agree to this condition. As soon as this slip is returned to School we will issue a replacement iPad.

Kind regards,

A. R. Anderson
VP Teaching and Learning

Please detach and return:

For the attention of Mr Anderson (VP Teaching and Learning):

My daughter _____ has damaged her School iPad and I understand that my daughter will be issued with a replacement iPad on the condition that, should she damage another School iPad, I will be liable for the full cost of its repair or replacement.

Signed (Parent / Guardian) _____

Date _____

Appendix 1 - iPad Return Form for leaving pupils

Before returning an iPad please provide the details requested below and sign to confirm the return of the iPad, School supplied iPad case and a working Apple branded charger power adapter.

Note: You should back up any files including photos and videos you want to keep from the iPad or cloud storage to a home computer. See the other side of this page for general backing up instructions.

*Remember when backing up to use **@c2ken.net** for OneDrive and Google Drive access*

Pupil School username _____**@c2ken.net** (please print)

Pupil name _____ (please print clearly)**Form Class** _____

Please tick

Returning a fully working iPad in the School provided case ☐

Returning a working Apple branded iPad charger power adapter ☐

Unreturned School iPad case and Apple branded iPad charger have a replacement fee of £10 for the cover and £19.00 for the Apple charger to be replaced.

Payment attached or missing item/s if applicable: Y / N

Condition of iPad Cover:

Please circle your answer **Ok / Broken**

Condition of iPad screen:

Please circle your answer **Ok / Noticeably Scratched / Cracked / Broken**

Other faults to note or comments:

_____

Parent / Guardian Signature _____ **Date** _____

Pupil Returner Signature _____ **Date** _____

Thank you for your cooperation

Pupils can speak to the ICT Support Officer at break time or lunchtime in the Learning Centre if assistance is required

School iPad return general back up instructions

Any files not backed up from the iPad or from any cloud storage system used in Strathearn School **before** the iPad is returned should be considered lost as the iPad will be wiped and cloud storage accounts closed when you leave.

How to back up iPad schoolwork

Most Apps allow for work to be uploaded to cloud storage. It is the iPad users' responsibility to save important work to cloud storage and not locally to an iPad.

If you need to remove Apps to gain some working space on your iPad, remember the Self Service App allows allocated apps to be reinstalled at a later date if required. **Back up work from Apps before removing them.**

*Remember we use **@c2ken.net** for access to Microsoft O365 Apps like OneDrive and Google Apps such as Google Drive. Use **@strathearnschool.org** for iCloud files.*

Back up any files you wish to keep by uploading them to OneDrive or Google Drive from within the Apps you have used. If these are not an option check for it under 'More'. Use the OneDrive cloud storage if Google Drive is not available. iCloud Drive may be available in some Apps for storing files but it is only recommended if Google Drive and OneDrive are unavailable. Once used an iCloud Drive shortcut can appear on your iPad with which to access the iCloud Drive files.

Look for the following icons in Apps to be able to copy files to a cloud based storage location:

Back up any photos and videos you wish to keep by uploading them to One Drive or Google Drive (use the Select option to select groups of photos then tap the page with an arrow pointing up at the top left of the screen and select the Drive you wish to use). You can also Airdrop to send photos and small videos to another Apple device.

OR note: It is also possible to copy any photos and videos you wish to keep from your camera roll by connecting the iPad to a home computer and copying them from the iPad to your computer.

Apple Apps such as Pages, Numbers, or Keynote documents can be backed up by, using the **3 DOTS** icon in the upper right hand corner, from the menu choose **Send a Copy**. Next select the format you'd like the document in, choose the required App, i.e. Google Drive then tap on the location where to save and tap on **Save Here** and finally tap **UPLOAD**.

Finally, to ensure you have a backup of these files access the used cloud storage website on a home computer and download the files to an appropriately named folder.

Please fill in, sign and date the form on the other side of this page and return it with the iPad in the School supplied case along with a working Apple iPad charger plug (*you may keep the lightning cable*).

Thank you for your cooperation

Pupils can speak to the ICT Support Officer at break time or lunchtime in the Learning Centre if assistance is required

Appendix II

Strathearn School

School Owned iPad and EA Portable Device: Staff Acceptable Use Policy (AUP) and Procedures

Review Date	Author
May 2022	L. Turner
Oct 2025	L. Turner

Acceptable Use Policy for Staff

This policy operates in conjunction with the E-Safety Policy and is designed to help and protect staff in Strathearn School.
The terms of acceptable use of an iPad and Apple TV, supplied by the School are:-

Administration and Security – School owned iPads

- The iPad remains the property of the School and can be recalled, by the School, at any time.
- Use of the iPad is for educational purposes only and all relevant school policies apply
- These devices are for the user's use only and must not be loaned out to any other party, including other staff, pupils, family members etc.
- Every precaution is to be taken to avoid damage to or loss of these devices.
- The School provided case or cover for the iPad must be used and kept on at all times. Any issues with the case or cover should be reported when noticed as a replacement may be required.
- Only the School's given Apple School Managed Apple ID's are to be used to sign into iCloud in the Settings App for backing up settings and storing schoolwork Files.
- The School iPads/EA Portable Devices are not to be used for BETA testing forthcoming operating systems.
- The School iPads must not be jailbroken
- iPads must be named after the member of staff by using their C2K username in the iPad name settings found in Settings>General>About>Name. This helps identify who is to receive which apps.
- The School iPads may not be linked with a personal Apple watch or Macbook or iMac
- Only approved members of staff may have access to social media to promote the School or for departmental educational use. School devices are not to be used for personal social media use.
- The iPad, charger and lightning cable must be stored in a secure place at all times when not in use.
- A security PIN of at least four digits must be used to secure the iPad and the auto-lock set to at least fifteen minutes.
- The security PIN of the device is held only by the user and never divulged to pupils, staff (unless for ICT Support or authorized by a member of SLT) or any other party including family members.
- When in School, the School provided filtered networks are to be used (C2KWireless). School devices are not to be connected to a hotspot or other non-filtered networks for protection.
- Before you leave the School, the device shall be returned signed out of iCloud and the PIN set to 1234

Administration and Security – EA Portable Device

- Ownership of this device rests with C2k, staff may retain it for School use while in the employment of Strathearn school.
- Logon to the device is only possible with a valid C2k Username and password, and that disclosure of individual C2k Username and password represents a security breach.
- The facility to install software should only be used to load resources which are licensed, and which are appropriate for School needs. In particular, device users may not install Windows updates or any hacking tools and should not switch off Windows firewall.

- The device is insured by C2k for thefts or malfunction and not for accidental damage. If the device is removed from School, reasonable care must be taken to ensure it is safely stored.
- Antivirus software is provided and automatically updated in School or when connected to the Internet. This protection must be kept up to date if the device has not been connected to the School network or the Internet for more than two weeks.
- The device may be used outside School for Internet use with any Internet Services Provider (ISP). It is the responsibility of device users to ensure that confidential information is not saved to the portable device.
- The device should not be given or lent or used by anyone other than the nominated member of staff when outside School.
- If the device is lost or stolen, the School should be notified immediately, or during School holidays, the C2k Helpdesk (08000 931 541).
- The device must be returned to School if the nominated member of staff ceases employment with the School.

Data Storage and Use

- Files stored on staff devices must not be regarded as private. The School reserves the right to monitor, review and examine content, internet history, usage, communications and files of users, and, where it deems it to be necessary, will intercept and delete material which it considers inappropriate, and prohibit the use of such material.
- Documents on staff devices should be backed-up regularly using online Cloud Storage capabilities.
- Only the C2K email account should be installed through the Mail or Outlook App on staff devices. Personal email can still be accessed but only through a web-browser such as Safari.
- Other personal items (for example, documents, audio, text, photographs, videos) which contravene School policies must NOT be stored on these devices.

Use of Digital Media

- The use of the device cameras must be in line with the School's E-Safety Policy and the Safeguarding and Child Protection Policy. Photographs should be cleared out regularly and not stored longer than necessary.
- The user is responsible for understanding and adhering to all policies and copyright requirements related to digital media and the use of the School allocated device.

Reporting Incidents

- In the case of loss, theft or other damage occurring outside of School, the ICT Support Officer must be informed as soon as possible. In consultation with the Vice-Principal (Teaching & Learning), it is the responsibility of the member of staff to follow School procedures in the event of the iPad needing repair.
- Issues with a staff device should be reported immediately to the ICT Officer Support

On receipt of an iPad/EA Portable Device, I understand and agree to abide by this Acceptable Use Policy. I further understand that should I commit any violation of this Policy, my access privileges may be revoked, school disciplinary and/or appropriate legal action may be taken.

This policy is subject to change. Updated policies may be found in the staff handbook.

User (PRINT): .....

Signed: .....

Date: .....

Appendix III

Strathearn School

Use of Personal Devices in School: Conditions and Agreement

Review Date	Author
Oct 2025	L. Turner

Introduction

Strathearn School recognises that internet enabled devices play an increasing role in today's society and can be valuable tools in an educational environment. While the School will continue to provide extensive ICT facilities including access to various computer suites and laptops in the 6th Form study, we understand that some pupils would prefer to work on their own personal laptop or tablet. This document sets out the conditions under which girls in 6th Form may bring their own devices into School to use on the School's wireless network. The aim of this policy is to enhance learning and achievement as well as to prepare them for the level of digital competency they will require in the world beyond School.

The School Network

By signing up to the terms of this agreement students can only bring devices into school if they are connected to the School's network which has filtered and monitored internet access. Students will be provided with instructions on how to access the network. No devices should be connected to any other network including through personal mobile device while in use at School

Conditions for use of the School wireless network:

1. Students can use their own devices to access internet-based resources during study periods. They may only be used during lessons with the explicit permission of the classroom teacher.
2. The purpose of personal devices at School is to support broader learning during lessons and independent study. Using the device for other reasons e.g. games, social networking sites or messaging, is not allowed.
3. Students must not use such devices to record, transmit, or post any of the following: photos, audio, or video of any person(s) within School without the explicit permission of the person or persons involved.
4. Students must not access/send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature (including existing material stored on the device).
5. Students must not copy material that is protected by copyright, without prior permission from the copyright owner.

School Liability

Students bring their devices to School at their own risk. They are expected to act responsibly with regards to their own device, keeping it up to date with virus software and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices. Strathearn School is not responsible
for:

- Personal devices that are broken while at School or during school activities
- Personal devices that are lost or stolen at School or during school activities
- Students must keep their devices in a secure place when not in use (e.g. a locked locker).

It is advisable to ensure that there is adequate insurance coverage to protect the device from any accidental damage, theft or loss. Please be aware that School staff will not provide any technical support on either hardware or software.

Consequences for abuse of this Agreement

If a student breaches these conditions, they will be dealt with in accordance with our Positive Behaviour Policy.

Breaches of conditions 1 and 2 will incur a misconduct 2(n), the device will be confiscated and placed in reception until 3.30pm that day. Breaching conditions 3 and 4 will incur a misconduct 3 (k and m) which will mean an automatic detention. The Principal reserves the right to review a sanction where the specific nature of the misconduct one which is not currently prescribed in our Positive Behaviour Policy.

Student Name _____Class_____

Parental Agreement

I permit my daughter to use her own internet enabled device at School for educational purposes only.

I have read and accept the conditions for allowing students in 6th Form to bring their own device to School. I understand that she will be wholly responsible for the security and maintenance of the device while she is in School/ involved in any school-related activity/travelling to and from School.

I am aware of the strict filtering system that operates on the School's network and that action will be taken if inappropriate material is detected on any device brought into School by a student.

Signed:_____ (Parent/Guardian)

Date: _____

Student Agreement

I have read and accept the conditions for allowing my use of my own device in School. I will adhere to these conditions and understand the consequences if I do not.

I understand that I will be wholly responsible for the security and maintenance of the device while it is in School/ involved in any School-related activity/travelling to and from School.

I am aware of the strict filtering system that operates on the School's network and that action will be taken if inappropriate material is detected on any device brought into School by a student.

Signed:_____(Student)

Date: _____