04.30 Online Safety Policy

Written by	Designated Safeguarding Lead
Date for Review	31January 2025
ISI Policy Code	
Scope of policy	EYFS, Pre Prep and Prep School

Introduction

This policy is a Whole School Policy and includes EYFS and Boarding.

It is the duty of Saint Ronan's to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking and abuse.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

This policy, supported by the Computer User Agreements (for all staff and Prep School pupils) is implemented to protect the interests and safety of the whole School community. All staff should be aware that pupils and staff are vulnerable online as they can be subject to cyberbullying and online exploitation. In this respect, the Online Safety Policy must be read in conjunction with the following policies:

- Safeguarding and Child Protection;
- Health and Safety;
- Behaviour Policy;
- Anti-Bullying (including cyberbullying);
- Mobile Phone Policy;
- Data Protection;
- PSHEE/RSE/SMSC

Management of Online Safeguarding

The DSL and Director of IT have responsibility for keeping up to date with current online safety issues and guidance. They will work to ensure that this policy is upheld by all members of the School community. Pastoral Leads and Deputy DSLs will provide a close link to the pastoral side of the School.

The DSL is ultimately responsible for online safety, including understanding the filtering and monitoring systems in place.

As with all issues of safety, all staff have a responsibility to keep the children safe and are encouraged to create a talking culture to address online safety issues and concerns which may arise in classrooms. All staff have a duty to use ICT safely and professionally themselves as well as to safeguarding pupils' usage. Whilst we would urge all staff to report concerns through the DSL, all staff can refer directly to the Education Safeguarding Advisor for advice should they feel this is appropriate.

All staff are expected to understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring. They should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face.

Saint Ronan's believes that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of School. We regularly promote online safety with parents and seek to engender a wide understanding of the benefits and risks related to internet usage. Through Computing lessons, PSHEE and various pastoral initiatives, children are taught about online safety. The school recognises that child on child abuse, including sexual violence and sexual harassment can occur online and that victims of abuse or SEND children may be more vulnerable and need a more personalised and contextualised approach.

Governance

The School Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This is carried out by the Safeguarding Committee, receiving regular information about Online Safety incidents and monitoring reports. The Safeguarding Governor carries the following responsibilities:

Regular meetings with the DSL: termly, alongside Safeguarding Committee meetings.

- Regular monitoring of online incident logs
- Regular monitoring of changes to filtering
- Reporting to relevant Governors' meetings

SAFEGUARDING :

KEEPING PUPILS SAFE ONLINE - WHAT ARE THE RISKS?

Types of unsafe behaviour online

There are four broad areas of risk relating to young people's activities online:

CONTENT: being exposed to illegal, inappropriate or harmful material

CONTACT: being subjected to harmful online interaction with other users; and

CONDUCT: personal online behaviour that increases the likelihood of, or causes, harm.

COMMERCE: risks online such as gambling, inappropriate advertising, phishing or financial scams

	COMMERCIAL	AGGRESSIVE	SEXUAL	VALUES
CONTENT (types of content pupils might see)	• Adverts • Spam	• Violent/hate material	• Pornographic and unwelcome sexual comments	• Bias • Racist and extremist content • Misleading info/advice and fake news • Body image and self-esteem
CONTACT (types of interaction which pupils may have online)	• Tracking • Harvesting personal Information	• Bullying • Harassment • Stalking • Peer-to-peer pressure	• Meeting strangers • Grooming • Adults posing as children • Online Child Sexual Exploitation	• Self-harm • Suicide • Unwelcome persuasions • Grooming for extremism
CONDUCT (types of behaviour a pupil might get involved in online)	• Illegal downloading • Hacking • Terrorism	• Bullying • Harassment • Radicalisation	• Creating or uploading inappropriate material including making, sending and receiving explicit images (consensual and non-consensual sharing of nudes and semi nudes and/or pornography, sharing other explicit images • Unhealthy/inappropriate	• Misleading information or advice • Encouraging others to take risks online • Sharing extremist views • Addiction • Sexual relationships
COMMERCE (exposure to risks on line)	• Gambling • Financial scams • Phishing		• Inappropriate advertising	• Encouraging risky behaviours online • Cybercrime

The School attempts to minimise CONTENT concerns through its filtering and monitoring systems (see Technical Information) and seeks to educate children about online safety to provide them with the tools to keep themselves safe from CONTACT and CONDUCT and COMMERCE issues.

The School does not allow the children to use mobile phones or Smart technology at School.

The School recognises that children with a particular skill or interest may stray into cybercrime.

Events occurring outside School will be dealt with as part of the Behaviour, Anti Bullying Policies and Safeguarding Policies. The School will communicate with and educate parents about online safety.

MANAGING ONLINE SAFETY CONCERNS

The School will manage Online Safety incidents as follows:

RECOGNISE

- Is it illegal or inappropriate?
- Whose responsibility is it to respond?

RESPOND

What do you know about the children involved?

- Age and vulnerabilities? Any power differentials, SEN, known to social care/early help?
- Are there any underlying issues? i.e., low self-esteem, difficulty managing friendships?
- What are their views/perceptions on the concern?

Is the behaviour harmful or undesirable?

- What is the impact on the child(ren) - what concerning behaviour is being seen?
- What are the issues with the behaviour? e.g., secrecy, impact, duration and frequency

Are there risks to others, including other family members?

If appropriate, what are the views of parents?

Is additional support required to enable parents to ensure children are safe?

Procedure

1. If a pupil, member of staff, parent, guardian or anyone else raises an online concern, follow the guidance for safeguarding, i.e.,

    - Do not promise confidentiality. If a child asks you to keep a secret, explain that in order for them to receive the help and support they need, it may well be necessary for you to speak to someone else.

- Listen carefully being non-judgmental, supportive and respectful.
- Ask to see evidence. If evidence is available, exercise caution in asking to view anything which may involve inappropriate images or videos.
- Preserve the evidence, for example by collecting the relevant device, but do not forward any illegal or inappropriate content as you could fall foul of the law in sending inappropriate content yourself. Staff should not print out, screen shot or in any way reproduce any material that could be considered inappropriate or illegal.

RECORD:

1. Wait until the end of the report and immediately record in writing (on CPOMS) the facts as the child presents them, plus any evidence as available and appropriate.
2. Do not include any personal opinions of the note taker.
3. Report your concerns to the DSL or in their absence the Director of IT or the Deputy DSLs.

REFER

1. If in doubt, consult with the Education Safeguarding Service.

- Do other agencies need to be informed? If so, who?
- Has a criminal offence been committed?
- Involve parents as appropriate and necessary - provide practical advice and support.

2. The School should consider whether this is an isolated incident or a systemic issue in the School.

- Apply sanctions in line with behaviour and safeguarding policies.
- Implement appropriate educational approaches.
- Consider if the wider community needs to be informed.

Any concerns about sexual abuse or serious/persistent emotional or physical abuse/harm should be referred. If in doubt, the DSL will consult with the Education Safeguarding Service. All members of staff can refer if needs be.

PUPIL EDUCATION

<u>Online Safety in the curriculum and School community</u>

The School:

- Encourages pupils to tell us when they have concerns about their online safety.
- Educates the children how to respond to harmful content online:
  - *Build and develop their self-esteem online*
  - *Develop practical online skills*
  - *Privacy setting, blocking, reporting, etc.*
  - *Look at alternative sites for support*

- *Enable them to search for advice safely online*
- *Do they understand bias and how to check if a source is safe and reliable*?

- To support the above and in addition to Curriculum time (directly through Computer Science and also through other subjects), the School provides regular and meaningful online safety guidance both formally (PSHEE and visiting speakers in) **and through pastoral assemblies.**
- The School can be reactive through Year group assemblies should any present and pressing online safety concerns need to be tackled in an age-appropriate manner.
- The School has set up peer listening groups involving the Y8 children who annually conduct assemblies on online safety, and also conduct question and answer sessions to the younger ones as required.
- All children will electronically sign a Computer User Agreement annually (see Appendix 1).
- Any staff member using Social Media sites as a teaching resource must ensure they have checked the link prior to playing, that they are present whilst the link is being played and are there to ensure the removal of the link in class if it is deemed inappropriate. If a cover teacher is uncomfortable with any links being played, they should stop them immediately.
- Occasionally children are asked to do research at home which may involve online resources; staff must be sure to guide the children carefully. The School will send out annual letters to parents advising them to ensure parental controls are in place, informing them how to report concerns online and to regularly check browsing history.

KEEPING STAFF SAFE ONLINE

- All staff electronically sign an Acceptable Use Policy (AUP) (see Appendix 2).
- This is updated and electronically agreed annually.
- Staff should be aware that their online conduct out of School could have an impact on their role and reputation within School. Civil, legal or disciplinary action could be taken if they are found to have brought the profession of the School into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- Staff are required to maintain the professional standards demanded of adults working in a School who, by virtue of their employment, are in a position of power, influence and trust. All staff are required to be familiar with the Staff Code of Conduct contained in the Safeguarding Policy. They should protect the reputation of the School and of themselves in the real and virtual world.
- If a member of staff discovers an online safety issue concerning pupils or staff, they should immediately contact the Director of IT or DSL.

Management of Social Networking, Social Media and Personal Publishing

1. All staff are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory, and they are reminded that what is posted online may be viewed by a large audience and may remain there forever.
2. Staff may have private social media accounts but may not be "friends" with, "follow" or in any other way engage with current or past pupils using private social media

accounts unless the person is an adult and has finished full time education. The IT Director makes this clear during staff induction meetings.

3. Staff members must ensure that their security settings are private, and private social media accounts need to be used in a manner that does not bring the staff or the School into disrepute or affect their professional status.
4. Staff must take particular care if they chose to make reference to the School in any private posts, that they do not make damaging statements which would adversely affect the reputation of the School.
5. Staff have a duty to behave in a professional manner, even in their private posts, as any information posted online could compromise their ability to discharge their duty as a member of School staff working with young people. Teachers in particular should be aware that the DfES's Teachers' Standards (2010) state that "a teacher is expected to demonstrate consistently high standards of personal and professional conduct".
6. If a member of staff wishes to set up an official blog or wiki, please refer to the School's media policy.
7. The school is committed to safeguarding staff from cyberbullying, including incidents that occur outside school. Any staff member experiencing online harassment should report it to the school leadership, who will provide support and guidance. Staff are encouraged to document incidents and may be advised to report serious cases to social media platforms, the police, or their union. If the perpetrator is a student, appropriate disciplinary action will be taken, and parents will be involved. If a parent or member of the public is responsible, the school may issue formal warnings, restrict access to school premises, or take legal action if necessary. The school will also promote awareness of cyberbullying through staff training and community engagement, ensuring a culture of respect and online safety.

Management of mobile phones and personal devices

Information and guidance are contained in the **Mobile Phone Policy** and the agreement of managing staff laptops is outlined in the **AUP**.

Management of E-mail

- The use of e-mail is an essential means of communication. In the context of School, e-mails should **not** be considered private and staff should not use them in a personal capacity as the contents of School e-mails remain the property of the School.
- The School gives many members of staff their own e-mail account for use for School business. It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered.
- The School may inspect induvial e-mails for "specific business purposes", including:

1. establishing the content of transactions and other important business communications;
2. making sure employees are complying with the law and with our internal policies;
3. preventing abuse of our telecoms system;
4. checking emails when employees are on leave
5. Accessing e-mails for legal or commercial reasons once the employee has left the School.

- All e-mail users are expected to use appropriate language in e-mail communication and not to write anything defamatory, unpleasant or untrue about another person. Staff must inform the DSL if they receive an offensive e-mail.
- No one should open attachments from an untrusted source.
- We advise staff that, wherever possible, they should not respond to e-mails from parents after 7pm or at the weekend.

COMPLAINTS

As with all issues of safety at Saint Ronan's, if a member of staff, a pupil or a parent/carer has a complaint or concern relating to online safety, prompt action will be taken to deal with it. Complaints should be addressed to the DSL or the Director of ICT in the first instance, who will undertake an immediate investigation and liaise with the leadership team and any members of staff or pupils involved. Please see the Complaints Policy for further information.

Appendix 1: Pupil Computer User Agreement

SAINT RONAN'S SCHOOL
Computer User Agreement

Saint Ronan's provides an extensive computer network for the use of both staff and pupils. To make sure that the computer network is used in a way which is acceptable to the School, all users must read and agree to the following points:

- **Your User Account**
  Your user account is to be used only by yourself. You must not tell other people your password or use other people's usernames to log on. You should not attempt to find out other people's passwords or to gain access to their user accounts. You are responsible for all activity which is traced to your user account regardless of who was using the account at the time. **If anyone has accessed your computer user account, you must tell your Form Tutor or Mr Clarke.**

- **Access to the Internet**
  Internet access is provided to be used as resource for your work and you should not pass off material downloaded from the internet as your own as this is plagiarism. You may only use the internet when you are being supervised by a member of staff or designated prefect. We will filter your internet connection to restrict access to websites which contain unsuitable material. **If you come across a website which contains material you think might be unsuitable, you should close the website and report it to a member of staff.**

- **E-mail**
  You are provided with an e-mail address as a method of communication within the School. You may also use your e-mail address to send work between home and School and, during boarding time, to keep in touch with people outside of School. You should not use your e-mail address to contact or reply to anybody you do not know or use it during lesson time. You should send e-mails to only one person at a time. You should not send offensive messages or pictures, use obscene language or use the e-mail to bully pupils, or annoy them.
  If you receive an offensive message, you should report it to your Form Teacher, Pastoral Head, Mr Clarke or Mrs George.

- **Photos and Videos**
  You may only take photos or videos with School-owned equipment unless specific permission has been given. You should not upload any photos or videos taken at School to any websites or social media, either from School or from home.

- **Common Sense**
  Above all, make sure you are using common sense to guide your use of the computer network. To protect all pupils, the School can access your files and e-mails.

If you abuse your access to the School's computer network you will be subject to the usual disciplinary procedures and may have your access to the computer network removed.

I have understood the above points on the use of the School's computer network.
Name:
Form:
Date:

Appendix 2:

SAINT RONAN'S SCHOOL

Staff Acceptable Use of ICT Policy [changed per declaration below] – *to be read in conjunction with the Online Safety Policy, Mobile Phone Policy and Staff Code of Conduct.*

All members of staff have a responsibility to use the School's computer system in a professional, lawful and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using ICT and the School's systems, they are asked to read and sign this Acceptable Use Policy to acknowledge acceptance of the terms therein and the contents of the Online Safety Policy.

Definition

I understand that ICT includes network, data and data storage, online and offline communication technologies, and access devices.

If I have any concerns, I will take these to the Director of IT.

Professional and Legal obligations

I understand that the computer misuse act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with the intent to commit or facilitate commission of further offences or to modify computer material without authorisation. I will therefore use the School's and any personal, ICT and information systems appropriately and within the law.

I will respect copyright and intellectual property rights.

My use of ICT and information systems will always be compatible with my professional role, whether using School or personal systems. This includes the use of e-mail, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will be in accordance with the School ethos and the law. It will not contain any inappropriate language nor any defamatory or libellous comments; it will not contravene the School's Equality Policy, e.g., in respect of gender, race, age, sexual orientation, religion or beliefs, or any other protected characteristic.

I will not create, transmit, publish or forward any material that is likely to harass or cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role in the School into disrepute.

I will report any accidental access to unsuitable websites, receipt of inappropriate materials, filtering breaches to the DSL or the Director of IT as soon as possible.

I will report all incidents of concern regarding children's online safety to the DSL or Director of IT as soon as possible. In their absence I will report any concerns to the deputy DSLs.

I will promote safe internet use with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

Security

I will respect system security and I will not disclose any password or security information.

To prevent unauthorised access to systems or personal data, I will not leave any device unattended without first logging out or locking my login as appropriate.

When I am away from School I will ensure that nobody gains access to the School network, systems or personal data via my username.

I will not attempt to bypass any filtering and/or security systems put in place by the School. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any School-related documents and files, I will report this to the Director of IT as soon as possible.

In the event of my not being in School e.g., through illness or if I have left the School, I understand that the School may access my folders and e-mail to recover important documents.

Our monitoring and filtering systems may result in your personal correspondence being seen by members of staff responsible for safeguarding. All e-mails sent and received by members of staff via the School's e-mail system are journalled, meaning that copies are kept regardless of them being deleted from your mailbox.

Data and Data Protection

I will ensure that any personal data of pupils, staff or parents is kept in accordance with the Data Protection Act 1998 and the European General Data Protection Regulations (GDPR) and images of pupils will be used in line with the School's Data Protection Policy and will always take into account parental consent.

I will not keep professional documents which contain School-related sensitive or personal information on any personal devices or on a cloud storage system, unless they are secured and encrypted.

I will protect the devices in my care from unapproved access or theft. I will not store any personal data on the School's computer system without the written permission of the Director of IT.

Where it believes unauthorised and/or inappropriate use of the information systems or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with the School's Online Safety Policy, The Mobile Phone Policy and the Staff Acceptable Use of ICT Policy.

Signed:

Print Name:

Dated:

Appendix 3: Pupil Laptop User Agreement

PUPIL LAPTOP POLICY

This is for children who are required by the school to use a laptop

Computers are recognised as a useful tool to help you in a variety of ways:

- You can be proud of your presentation - the typeface does not deteriorate with speed or tiredness.
- It will be easier to edit your work - no messy crossing out!
- You are free from the purely mechanical aspect of writing. This will allow you to express your ideas more fluently and with greater ease.

Your teachers are very happy for you to use your laptop in their lessons and for producing all written homework tasks. However, it is essential you follow these simple requirements:

- Your laptop MUST be fully charged. It is your responsibility to charge it at home overnight.
- You must have a password set to access your laptop and you must keep this to yourself; other pupils are not to use your laptop.
- Your laptop is for use in lessons and for completing preps. It is NOT an entertainment device.
- Your teachers will make it clear if they expect you to bring your laptop to a lesson.
- It is your responsibility to save all work on your laptop appropriately.
- It is your responsibility to hand in your preps on time.
- You should print out work done in a lesson immediately.
- You must make sure that your laptop is on mute and all recording devices are disabled.
- You are allowed to use only authorised software and may not use your laptop to access the internet.
- This code of practice is in addition to the School Computer User Agreement.

By signing this code of practice you are agreeing to follow these basic requirements so that your laptop will be a help rather than a hindrance, both to yourself and to your teachers.

Name:	_____
Signature:	_____
Date:	_____

Appendix 4: Parent guidelines on Laptop use

- A pupil needs an Educational Psychologist's report recommending the use of a laptop.
- Parents must ensure that the pupil has reached the required standard in touch typing and laptop use as set out by the School or is embarking on some keyboard/touch typing training.
- Use of pupil's own laptop in School is understood to be at the parents' risk and therefore it is recommended that parents ensure that the laptop is securely named and appropriately insured.
- Pupils may use School laptops designated for exam use (they may not use their own). They will not be able to use spell checker. Exam papers will be collected on a memory stick and handed to the adjudicator.
- Other than exams it is the responsibility of the pupil to print out work.
- Parents must respect the teacher's choice of work mode whether laptop use, sheets, WriteOnline, handwriting, etc.
- Parents and children must ensure that laptops are fully charged for the start of each School day.
- All laptops must be checked by the Director of IT before being used at School to ensure they have up-to-date and appropriate commercial security software installed. If they do not, parents will be asked to acquire some as soon as possible.
- Parents are responsible for maintenance of their child's laptop including any repairs and updates. The IT Department will offer day-to-day support to pupils in School.
- Any additional or specialist software required by a pupil (e.g., recommended by an Educational Psychologist) is the responsibility of the parents to acquire.

Appendix 5:

Even the most robust filtering and monitoring systems will not be 100% effective at eliminating risk to children. Our filtering and monitoring systems are members of the Internet Watch Foundation.

Technical Information

Filtering

Internet access is filtered by Watchguard, which is a next-generation firewall and is CIPA compliant. The filter blocks access to websites known to be age inappropriate, known to host malware, or falling within categories that the School has restricted (for example, social networking). The Watchguard database of websites is updated automatically several times daily. All web browsing activity is logged by the firewall.

Monitoring

Use of computers by children is monitored using Senso. Senso detects keypresses as users type, and identifies matches for 'trigger' keywords, phrases or abbreviations. Senso also scans the titles and content of websites. The keyword libraries are developed in partnership with the UK Government and specialist organisations. The libraries provide definitions relating to a broad range of safeguarding issues, from bullying and trolling to grooming, self-harm, sexting and counter-radicalisation, as specified in KCSiE.

Reports of activity are monitored in real time by the Safeguarding Team. Each report includes a screenshot or a short video and a history of the child's activity prior to the trigger point. If necessary, investigation is then carried out with the pupil concerned.

Senso also provides a 'Report a Concern' button where pupils can access help from staff if they have a concern.

In exceptional circumstances, the School will access files and e-mails to protect the interest of staff and pupils as well as the School's reputation. This will only be done with the permission of a member of the SMT.

Password Management for staff

Staff must obtain a unique key to register their devices with the School's Wifi system.

Staff are issued with a temporary password on arrival and they are advised to change it as soon as possible. Passwords must have a minimum of 8 characters and they must contain a combination of at least 3 of the following:

- Upper Case character
- Lower case character
- Numbers 0-9
- Special character

Passwords may not contain the user's account name or display name.

Password Management for children

Year	Format	Example
1 & 2	Three lower case three-letter words joined by a full stop. All accounts in each year share the same password.	hat.car.sun
3	Three lower case three-letter words joined by a full stop.	jug.ear.ant
4	Three mixed case three-letter words joined by a full stop.	Box.Top.Fun
5	Three mixed case three-letter words joined by a variety of symbols (+, &, *, !)	Log+Ice!Cat
6, 7, 8	Three mixed case four-letter words joined by a variety of symbols	Heat&Blue*Buzz