'Working together in the light of Christ"

UK Council for Internet Safety

SWGfL

Introduction to Online Safety Policy

Our online safety policy will operate in conjunction with other policies including those for pupil behaviour, anti-bullying, curriculum, data protection and security. It involves all members of staff from the Headteacher to any new member of staff. Through its compliance it will ensure that everyone knows and understands their responsibilities and can act upon them.

Online safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The policy is specific to St Mary's Catholic Primary School and adheres to guidelines set by SWGfL regarding online safety and The UK Council for Internet Safety's 'Digital Resilience Framework' and 'Education for a Connected World – A framework to equip children and young people for digital life'.

Who are SWGfL?

The South West Grid for Learning Trust is an educational trust that has an international reputation in supporting schools with online safety. SWGfL, along with partners Childnet and IWF, launched the UK Safer Internet Centre (UKSIC) in January 2011 as part of the European Commission's Safer Internet Programme. SWGfL is a founding member of UKCCIS (UK Council for Child Internet Safety) and has spoken at conferences across Europe, America and Africa. More information about its wide ranging eSsafety services for schools can be found on the SWGfL website – www.swgfl.org.uk.

Schedule for Development, Monitoring and Review

This e-safety policy was approved by the Local Governing Body of the School on:	
The implementation of this online safety policy will be monitored by:	Online Safety Champion (Clive Lakatos) and the Senior Leadership Team.
Due Date for next review:	3 years
Availability of the Policy:	The policy can be viewed online via the school website: https://www.sjcpschool.co.uk/. A paper copy is displayed on the Health and Safety Notice Board in the School Staff room.
Should serious online safety incidents take place, the following external persons / agencies should be informed:	SSCT (Safer School Community Team) See also Appendix A. Email: ssct@dorset.pnn.police.uk
The School will monitor the impact of the Policy using:	• Logs of reported incidents • Surveys / questionnaires of pupils and staff. • Audits will be carried out annually by Online Safety Champion (C Lakatos) and the Senior Leadership Team. See Appendix C.

Rationale

At St Mary's children fully enjoy safe areas of the internet and the amazing opportunities that a connected world brings. They develop a critical awareness of their own, and others', online behaviour and have strategies to stay safe and make a positive contribution online.

However, use of technology has become a significant component in Child Exploitation, Sexual Predation and Radicalisation and an effective approach to online safety to empower pupils and staff to protect and educate the whole school community in their use of technology is essential. At St Mary's this strategy has four stages: Prevent, Identify, Intervene, Escalate (See 'Referral Process – Appendix A').

We have identified three key areas of risk:

1) Content (illegal, harmful or inappropriate, fake news, racism, radicalism and extremism.

2) Contact- harmful online interaction with others (commercial advertising (pop-ups), grooming etc.)

3) Conduct- personal online behaviour: making and receiving online bullying, sending and receiving explicit images ('Youth produced sexual imagery'.)

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access. Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Improve Pupil Learning?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Plymouth CAST; access to learning wherever and whenever convenient.

How do teachers impact on pupil use of internet?

- Pupils will be taught what Internet use is acceptable and what is not as part of 'Ten:Ten Life to the Full' Relationships and Health Education (RHE) curriculum (see Appendices E and G) and given clear objectives for Internet use. This is enhanced further with lessons taught using Project Evolve.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation as part of Computing lessons (see Appendix F).
- Internet access will be planned to enrich and extend learning activities.
- Staff guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.

Authorised Internet Access

- All staff, trainee teachers and Governors must read and sign the 'Acceptable Information Use Agreement' (Appendix D) before using any school ICT resource.

- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to return a form if they wish to deny pupil access on-entry to Foundation Stage. A copy is available from the school office.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the network managers (AUX Solutions).
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown (see Appendix G) and how to validate information before accepting its accuracy (see Appendix F).

Staff and Governor Email

- All staff and Governors have a school based email account.
- Staff may only use approved e-mail accounts on the school system.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully before sending, in the same way as a letter written on school headed paper, proof read by SLT.
- The forwarding of chain letters is not permitted.

Social Networking (see separate guidelines for Social Networking use)

- Not to be used in school or using school equipment.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils are told not to access any social network sites. Awareness of minimum age for common social networking sites is explicitly taught as part of RHE curriculum (see Appendix E) and half-termly Online Safety themed Base Assemblies.
- Pupils are to be advised on security and encouraged to set strong passwords, deny access to unknown individuals and how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.

Filtering

The school sets up their own filtering with **RM SafetyNet** and will work to ensure filtering systems are as effective as possible.

Managing Emerging Technologies

- Emerging technologies are examined for educational benefit and a risk assessment carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time.

Published Content and the School Web Site

- The contact details on the School Website are the school address, e-mail and telephone number. Staff, Governor or pupils personal information will not be published.
- The Head Teacher and Network Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.
- See CAST privacy notice on school website.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images. However, the school reserves the right to not allow photography or recording of particular school events.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Parents will be asked to sign a form giving permission to use their child's image on the school website as part of their enrolment.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

The GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

Information System Security

- School ICT systems capacity and security are reviewed annually.
- Virus protection is installed and updated frequently.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Plymouth CAST can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

Handling online safety Complaints

- A senior member of staff will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the Headteacher. A copy of the school's complaints policy is available on the school website.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Communication of Policy

Pupils

- Pupils are informed that Internet use is monitored.
- Each pupil in school receives an update and refresher of Online Safety rules (See Appendix B) every half-time in a dedicated base assembly. The aim of the update is to ensure that each pupil has a good understanding of research skills (avoiding plagiarism and upholding copyright regulations), understands the importance of reporting abuse and misuse, and adopts good online safety practice when using digital technologies both inside and outside of school.

Staff and Governors

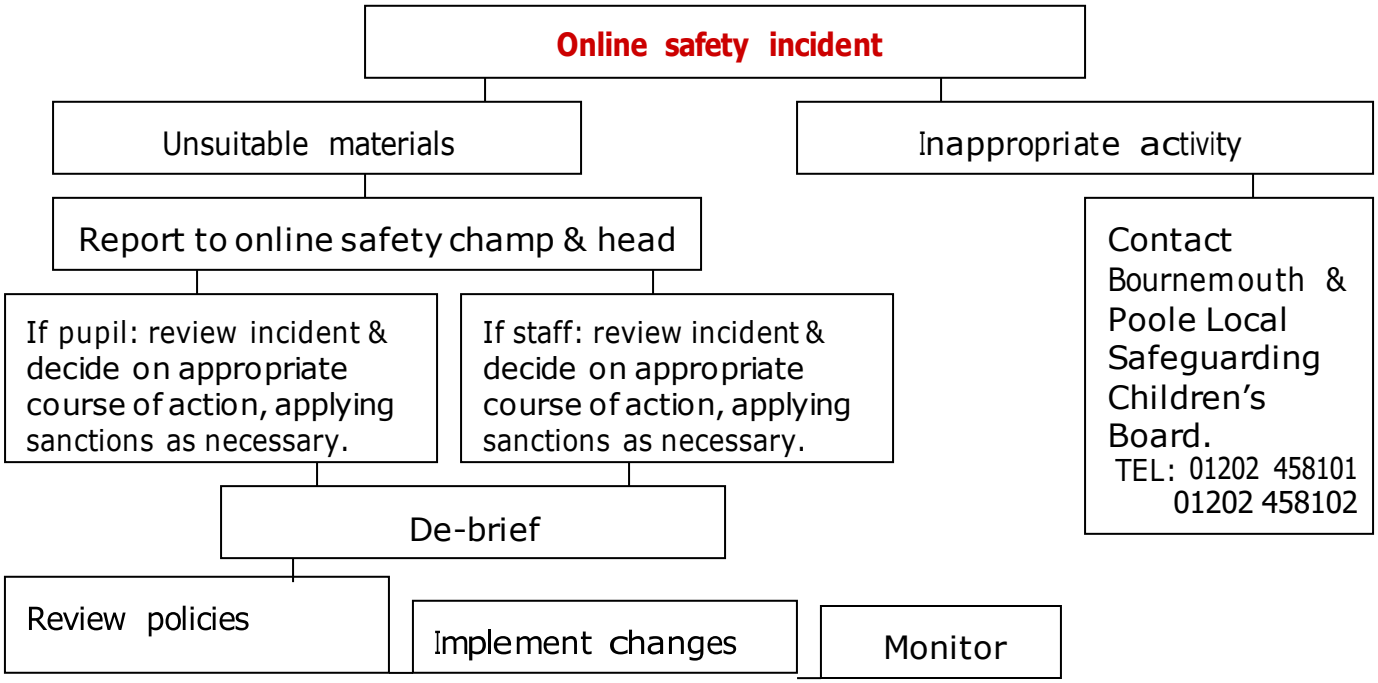
- All staff and Governors are given access to the School Online Safety Policy as part of their induction when they join the school. A paper copy of the Policy is displayed on the Health and Safety Notice board in the staff room.
- Staff and Governors should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. See Appendix B.

Parents

- Parents play a crucial role in ensuring that their children understand the need to use both the internet and mobile devices in an appropriate way. The school will take every opportunity to make them aware of the School Online Safety Policy via newsletters, the school Prospectus and the school Web site.

Appendix A - Referral Process

Flowchart for responding to online safety incidents in school.



Adapted from BECTA - Online safety 2005

Appendix B - Online Safety Rules

Adapted from https://beinternetawesome.withgoogle.com/en_uk/. Children in KS1 focus solely on 'When in doubt, discuss' to give them an early, simple and clear message that they must keep their trusted adults informed about their activities online at all times.

Think Before You Share

I will thoughtfully consider what I share and with whom, and keep extra-sensitive information to myself (such as my home address, current location, or other people's business).

Check it's For Real

I will watch out for phishing and scams, and report questionable activity every time.

Protect Your Stuff

I will take responsibility for protecting important information by crafting strong and unique passwords with characters, numbers, and symbols.

Respect Each Other

I will spread positivity and use the skills I have learned to block and report negative behaviours.

When in Doubt, Discuss

I will use my voice when I notice inappropriate behavior and seek out a trusted adult to discuss situations that make me uncomfortable. Because that's what it takes to be a safe and fearless explorer of the online world.

Appendix C - Online safety Audit

Good Habits

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Virgin. RM CensorNet will be used for the effective management of content filtering.

Online safety Audit

Has the school an online safety Policy that complies with CYPS guidance?	Y/N
Date of latest update: The Policy was agreed by governors on: The Policy is available for staff at: And for parents at:	
The DSL is Simon Thomas. Deputy DSLs are: Clive Lakatos, Bernie Wright. The online safety Champion is Mr Lakatos	
Has online safety training been provided for both pupils and staff?	Y/N
Do all staff sign an Acceptable Use form on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School online safety Rules?	Y/N
Have school online safety Rules been set for pupils?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	Y/N
Has the school filtering policy has been approved by SMT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N

Appendix D - Staff Acceptable Information Use Policy

Staff and Governor Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's online safety policy for further information:

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data (in paper or electronic format) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Sensitive electronic data will be encrypted if taken off site.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school online safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

Staff have been made aware that breaches of this code of conduct that, for example, result in a child's personal details coming into the public domain, may be investigated by the Information Commissioner and may result in a substantial fine of up to five million pounds.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

	Staff and other adults			Pupils	
Communication Technologies	**Not allowed**	**Allowed out of teaching time**	**Allowed at certain times**	**Not Allowed**	**Allowed with staff permission**
Mobile phones may be brought to school		✓		✓*	
Use of mobile phones in lessons	✓			✓	
Use of mobile phones		✓		✓	
Taking photos on personal mobile phones / cameras	✓			✓	
Use of other mobile devices eg tablets, gaming devices		✓			✓
Use of personal email addresses in school, or on school network		✓		✓	
Use of school email for personal emails	✓			✓	
Use of messaging apps			✓		✓
Use of social media			✓		✓
Use of blogs			✓		✓

***Must be handed in to the office in office / staffroom spaces only**

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …….. Print Name: …… Date: ……

Appendix E- Year 5 Spring Term 'Life to the Full' RHE Lesson: Is sharing always caring?

Sharing ONLINE

Knowing When It's OK and When It's Not

The internet is great for communication, information and entertainment! Write down what your favourite things are to do online:

.....

.....

.....

.....

.....

.....

.....

.....

.....

But just like in the real world, we need to take steps to keep safe in the digital world. Write down the age limits for the following websites or social media apps:

Facebook: ..... Twitter: ..... Instagram: .....

Snapchat: ..... WhatsApp: ..... Youtube: .....

(turn the page) ->>

Appendix F- Year 4 Autumn Term Computing Lesson Slides: Can you believe everything you read online?

Activity 2

Read all about it!

Why do people create or share false information?

Think, pair, share

Activity 2

Did you think of any of these?

- To make money
- To be popular
- To gain power
- By mistake

Appendix G - Year 3 Spring RHE 'Life to the Full' Assessment Activity

Keeping SAFE

Name.....

Here is a conversation between two friends: Donna and Alisha.

Alisha I was playing **FightClub** last night.
Donna Are you allowed? My Dad won't let me play that.
Alisha Well no, I'm not allowed either but Mum and Dad were out and my brother was in charge and he was on the phone to his friends so no one knew.
Donna Oh, right.
Alisha And while I was playing, a box popped up on the screen and I clicked it. But then I wasn't playing **FightClub** anymore and there were messages appearing on the screen and I didn't know what to do.
Donna What did you do?
Alisha I shut the lid and went to my room.
Donna Does your brother know about it?
Alisha No, I didn't tell him.

What advice would you give to Alisha?
Write in the box what you think she should do now.