E-Safety Policy

September 2018

St. Osmund's Catholic Primary School

Approved:	**1st September 2018**
Review Timescale:	**Biennially**
Review:	**September 2020**
Reviewed by:	**Headteacher**

St Osmund's Catholic Primary School

Love for God ~ Love for Each Other ~ Love for Learning

Background/Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Our E-Safety policy helps to ensure safe and appropriate use. The development and implementation of this strategy involves all the stakeholders in our children's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that our E-Safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).
As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, 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 these risks.

1. Leadership and Management of E safety

The school E-Safety policy will feature as part of the review process within the School Improvement Plan. It will relate to other policies including those for behaviour, for personal, social and health education (PSHE), for bullying and safeguarding.

Our E-Safety Policy has been written by the school, building on the Wiltshire E-Safety template policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

1.2 Roles and Responsibilities

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the school

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports.

The role of the Child Protection and Safeguarding Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of E-Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to Curriculum Committee

Head Teacher

- is responsible for ensuring the safety (including E-safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator who, at St Osmund's is the Computing leader.
- is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- ensures that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- receives regular monitoring reports from the E-Safety Co-ordinator.
- should make SLT and governors aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.

Computing Leader

- leads on E-Safety in the school.
- takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies and documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- provides training and advice for staff.
- liaises with the Local Authority.
- liaises with school IT technical staff.
- receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments.
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors.
- reports regularly to Senior Leadership Team.

Network Manager / Technical staff:

The Network Manager / Systems Manager / ICT Technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets the E-Safety technical requirements outlined in the SWGfL Security Policy and Social Media and Networking Policy (SM&NP) and any relevant Local Authority E-Safety Policy and guidance.
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- SWGfL is informed of issues relating to the filtering applied by the Grid.
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant.
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator and Headteacher for investigation.
- that monitoring software and systems are implemented and updated as agreed in school policies.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of E-Safety matters and of the current school IT Acceptable Use Agreements, policy and practices, and abide by their contents.
- they have read, understood and signed the school Social Media and Networking Policy.
- they report any suspected misuse or problem to the Computing Leader or Headteacher for investigation.
- digital communications with students (email / School Website) should be on a professional level and only carried out using official school systems.
- E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- pupils understand and follow the school E-Safety and acceptable use policy.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor ICT activity in lessons, extra-curricular and extended school activities.
- they are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

All staff are responsible for ensuring that:

- The Laptop and iPad Acceptable use policies are adhered to (copied for information below):

While the laptop is in your care the following points must be noted:

1. The laptop remains the property of St Osmund's Catholic Primary School and is only for the use of the member of staff to whom it is issued (i.e. not their family members). It must be returned to the school in an acceptable condition if and when that member of staff leaves the school's employment.

2. Insurance cover provided by the school only applies when the laptop is in school. Once you leave the school grounds, the laptop is not insured by the school. You are responsible for any loss or damage incurred at home.

3. Only software licensed by the school, authorised by the Computing Leader (Grace Hooper, or the School's IT Technician Service/ Approved Senior Member of Staff) and installed by, or with the permission of the Computing Leader may be used.

4. Anti-virus software is installed and you are expected to check it is updating on a weekly basis. The Computing Leader can advise/remind staff of this procedure.

5. Do not remove any programs installed on the laptop.

6. When using the laptop at school or away from school, the Acceptable Use Policy for Staff applies.

7. Any faults with laptops must be reported to the Computing Leader as soon as possible. Under no circumstances should staff attempt to repair suspected hardware or software faults. These are to be carried out only under the terms of the warranty.

8. Training in the use of the laptop, how to access the network, Internet and e-mail will be provided by the Computing Leader/Technician Service.

9. Where remote access to the school network is available it is vital to log off when finished and to protect log-in details. This is to avoid unauthorised access to sensitive or shared material and to protect the school network from outside access by unauthorised users.

10. Any usage charges incurred by staff accessing the internet from home are not rechargeable to the school.

11. Within two weeks of the issue of a replacement laptop, the original laptop must be returned to the Computing Co-ordinator with 'My Documents' cleared and any additional programs added by the user removed. The original laptop may be re-issued to another adult or pupil user.

12. The laptop may be recalled for periodic maintenance, with appropriate notice given.
13. I will only use the school's hardware / email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body. For example, the school's ICT equipment at home may be used for personal interest of an acceptable nature; however, **staff must use their professional judgement at all times**.

14. The user will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory, and will ensure that online activity, both in school and outside school, will not bring the user's, or the school's, professional role or reputation into disrepute.

15. I will ensure that personal data (such as data held on MIS SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

16. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory, and will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. See also Wiltshire CC Social Media Policy.

Acceptable Use Policy for School iPads (including Loan Agreement for School iPads)
Your school iPad is on loan to you while you remain employed by St Osmund's Catholic Primary School.

While the iPad is in your care the following points must be noted:

1. The iPad remains the property of St Osmund's Catholic Primary School and is only for the use of the member of staff to whom it is issued (i.e. not their family members). It must be returned to the school in an acceptable condition if and when that member of staff leaves the school's employment.

2. Insurance cover provided by the school only applies when the iPad is in school. Once you leave the school grounds, the iPad is not insured by the school. You are responsible for any loss or damage incurred at home.

3. Only software licensed by the school, authorised by the HT, or the School's IT Technician Service/ Approved Senior Member of Staff) and installed by, or with the permission of the HT may be used.

4. Do not remove any programs originally installed on the iPad.

5. When using the iPad at school or away from school, the Acceptable Use Policy for Staff applies.

6. Any faults with iPads must be reported to the HT as soon as possible. Under no circumstances should staff attempt to repair suspected hardware or software faults. These are to be carried out only under the terms of the warranty.

7. Training in the use of the iPad, how to access the network, Internet and e-mail will be provided by the HT/Technician Service.

8. Any usage charges incurred by staff accessing the internet from home are not rechargeable to the school.

9. Within two weeks of the issue of a replacement iPad, the original iPad must be returned to the HT with 'Documents' cleared and any additional programs added by the user removed. The original iPad may be re-issued to another adult or pupil user.

10. The iPad may be recalled for periodic maintenance, with appropriate notice given.

11. I will only use the school's hardware / email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body. For example, the school's ICT equipment at home may be used for personal interest of an acceptable nature; however, **staff must use their professional judgement at all times**.

12. The user will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory, and will ensure that online activity, both in school and outside school, will not bring the user's, or the school's, professional role or reputation into disrepute.

13. I will ensure that personal data (such as data held on MIS SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

14. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory, and will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. See also Wiltshire CC Social Media Policy.

Safeguarding Team should be trained in E-Safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate on-line contact with adults / strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

1.3 How will Internet access be authorised?

- Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. Parental permission should be sought at least at the start of each Key Stage. SWGfL proactively monitors Internet usage for illegal (attempted access of child abuse and incitement for racial hatred) websites and will notify the local police and Wiltshire Council in these instances.
- The school will grant Internet access to all staff and pupils. A record will be kept, for instance, if a pupil's or staff member's access is withdrawn and the reasons for it.
- The school's GDPR consent forms will include permissions for video, sound and images for web publication.
- Visitors must apply for Internet access individually by agreeing to abide by the Acceptable Use Policy statement that is signed by all staff with school devices.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials. Parents will be informed that pupils will be provided with supervised Internet access.

1.4 How will filtering be managed?

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of St Osmund's community from youngest pupil to staff.

- A log of all staff with unfiltered access to the Internet will be kept and regularly reviewed.
- Computing leader will review the popular permitted and banned sites accessed by the school.
- The school will work in partnership with parents; Wiltshire Council, DFE and the SWGfL to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider (SWGfL) via the E-safety lead.
- Website logs will be regularly sampled and monitored.
- ICT coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the Internet Watch.

1.5 How will the risks be assessed?

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. St Osmund's Catholic Primary School will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

2 Teaching and Learning

2.1 Why is Internet use important?

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

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

2.2 How will Internet use enhance learning?

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- 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 networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.

2.2 How will pupils learn to evaluate Internet content?

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.
Ideally inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the South West Grid for Learning and recorded in the incidents log.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

3. Communication and Content

3.1 Website content

Publication of any information online will always be considered from a personal and school security viewpoint. Sensitive information may be better published in the school handbook or on a secure online area which requires authentication. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

- The point of contact on the school website is the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Photographs will be selected carefully.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- The nature of all items uploaded will not include content that allows the pupils to be identified.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website complies with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.2 Managing e-mail

E-mail is an essential means of communication for staff. However, the use of e-mail requires appropriate safety measures.

- Staff will use official school provided email accounts.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

3.3 On-line communications, social networking and social media.

On-line communications, social networking and social media services are filtered in school by the SWGfL but are likely to be accessible from home.

All staff are made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They are made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. This should be read alongside the **Staff Code of Conduct** and the **Social Media and Networking Policies**.

See below:

1. **Communication with Children** (Including Use of IT and Social Media)

In order to make best use of the many educational and social benefits of new and emerging technologies, pupils need opportunities to use and explore the digital world. E-safety risks are posed more by behaviours and values than the technology itself. Adults should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used.

All Adults Should:	**All Adults Must NOT:**
* Always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others *Work and be seen to work, in an open and transparent way *Support children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice *Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use *Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken *Support safer working practice *Minimise the risk of misplaced or malicious allegations made against adults who work with children and young people *Prevent adults abusing or misusing their position of trust *exercise reasonable and proper judgement when putting personal information onto social networking sites, such as addresses, home and mobile phone numbers	*Betray confidentiality agreements *Make a 'friend' of a child or young person where they are working on their social networking page, and should not become 'friends' with children or young person no longer receiving a service *Use or access social networking pages of children and young people and should never accept an invitation to become a 'friend' of a child or young person *Post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the agency into disrepute or could reflect negatively on their professionalism *Give their personal mobile numbers or personal e-mail addresses to children/young people or families - unless the need to do so is agreed with senior management and parents/carers *Request, or respond to, any personal information from a child/young person, other than that which might be appropriate as part of their professional role. Should staff be approached, they should inform their line manager *Accept requests to connect with pupils and ex-pupils. Where this has been requested the adult should inform their manager who will decide whether to discuss with the child's parents/carers

4. Monitoring / Review

Date on which this e-safety policy was approved	*See page 1*
Who will monitor the implementation of this e-safety policy?	*Computing leader* *Computing governor* *Curriculum Committee*
How often will the impact & effectiveness of the policy be monitored?	*Annually*
How will the impact & effectiveness of this policy be monitored?	• *Logs of reported incidents* • *SWGfL monitoring logs of internet activity (including sites visited)* • *Surveys / questionnaires of* ○ *pupils (e.g. Ofsted "Tell-us" survey / CEOP ThinkUknow survey)* ○ *parents / carers* ○ *staff*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*See page 1*
Should serious e-safety incidents take place, the following persons / external agencies should be informed:	• *Head teacher and Senior Leadership team,* • *LA ICT Manager,* • *LA* • *Safeguarding Officer, Police Commissioner's Office*