ST MARY'S CATHOLIC PRIMARY SCHOOL

E-SAFETY POLICY

DATE OF APPROVAL	**12/2018**
VERSION DATE	**V.01**
DATE UPLOADED	**12/2018**
DATE FOR REVIEW	**12/2019**
OWNER	**F&R Committee**

Introduction

This School policy is based on the model provided by the Wiltshire Learning Trust. Its purpose is to safeguard all in the School that use or have access to the internet for learning or administration.

It is the responsibility of the Headteacher to ensure that on a daily working basis the Internet policy is implemented and compliance with the policy monitored.

Leadership and Management

1. Authorised Access

Internet access for pupils is an essential resource for staff and children's learning. All children are given internet access as part of the taught curriculum. Should any parent do not wish their children to use the internet, they must inform the School in writing.

At KS1, access to the Internet will be by adult demonstration with access to specific, approved online materials. At KS2, parents will be informed that pupils will be provided with supervised Internet access. A copy of the information letter is at Appendix A.

2. Publication of material

No member of the School community – governors, staff employed in any capacity, or children - shall publish specific and detailed private thoughts about the School, especially those that may be considered threatening, hurtful or defamatory.

Parents wishing to photograph or video at an event should be made aware of the School's expectations and be required to comply with the School's Responsible Internet Use Agreement (Appendix B) as a condition of permission to photograph or record.

The School will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law.

3. Filtering and Monitoring

The School's Internet Service Provider (ISP) is OAKFORD TECHNOLOGY LIMITED. This has a service which proactively monitors Internet usage for attempts to access illegal (child abuse and incitement for racial hatred) content and will notify the local police and Wiltshire Council in these instances. If an illegal website/content is accessed, Netsweeper (the filtering service) notes this and reports it to the Internet Watch Foundation (IWF). IWF decides whether it is a police matter or not. Based on a category list of content IWF which does not publicize and is only accessible by the IWF, Oakford Technology is contacted who then contact the School.

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 the school community from the youngest pupil to staff.

The School will work in partnership with parents, Wiltshire Council, DFE and its ISP to ensure systems to protect pupils are reviewed and improved.

Should staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the School Office, and the School Business Manager will inform the ISP.

Website logs will be sampled and monitored periodically by the Headteacher and Deputy Headteacher.

Any material that the School believes is illegal, or may place an individual at risk must be referred to the appropriate authorities, including the Local Area Designated Officer (LADO), Police and the Internet Watch Foundation.

4. Risk

The Internet can raise educational standards, promote pupil achievement and ensure their wellbeing, support the professional work of staff and enhance the School's management information and business administration systems.

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. The School recognises that there is always a risk that unsuitable material may be available via the School's internet system, but will take all reasonable precautions to limit the risk.

Neither the School, Wiltshire Council, or Diocese accept liability for the material accessed, or any consequences of Internet access.

The use of computer systems without permission or for inappropriate purposes constitutes a criminal offence under the Computer Misuse Act 1990.

Teaching and Learning

5. The Curriculum

The Internet is an essential resource to support teaching and learning. Computer skills are vital to access life-long learning and employment; computing is now widely accepted as an essential life-skill. The statutory curriculum requires pupils to be responsible, competent, confident and creative users of information and communication technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology, such as web-based resources, e-mail and mobile learning.

6. Enhancing Teaching and Learning

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient.
- Access to a variety of worldwide educational resources.
- Inclusion in the National Education Network which connects all UK schools.
- 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.
- Educational and cultural exchanges between pupils worldwide.

7. Evaluating Content

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. It may be difficult to determine its origin and accuracy, as contextual clues may be missing or difficult to read. A whole curriculum approach may be required. The evaluation of online materials is part of teaching and learning in every subject, and will be viewed as a whole-school requirement across the curriculum.

- Pupils will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy. Pupils using the Internet outside of the School need to learn how to evaluate Internet information and to take care of their own safety and security. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

- Pupils will use age-appropriate tools to research Internet content.

Should staff or pupils discover an unsuitable site, or content they consider to be inappropriate, the URL (address) and content should be reported to the Headteacher or School Business Manager and then to the ISP.

Communication and Content

8. Website Content

The School's website is an important form of communication with its stakeholders, including children, parents, agencies, donors and other supporters, and the public. Publication on it of any information must always be considered from a standpoint of safeguarding and GDPR security viewpoint.

- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

- The point of contact on the school website is to be the School address, School e-mail and telephone numbers. Staff or pupils' personal information will not be published.

- The nature of all items uploaded will not include content that allows the pupils to be identified by name, either individually or through aggregated pieces of information.

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

- Written permission for photographs of pupils to be published on the school website is to be sought from individuals, parents or carers when the children start school. Photographs will be selected carefully to ensure they are appropriate.

9. Managing email

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

- It is School's policy that children shall not have access to email accounts on the School system

- Staff must use official school provided email accounts for all professional communications.

- Email sent to an external organisation should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on School headed paper.

10. On-line communications and Social Media

All staff are to be aware of the potential risks of using social networking sites for personal communications, either professionally with students or personally.

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the School's *Safer Working Practice* Policy.

- Staff are to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

- In line with *Guidance for Safer Working Practice for Adults who Work with Children and Young People*, it will not be considered appropriate for staff to engage in personal online communications with children and young people connected with the School.

- All staff are required to use professional judgement where they have friendships with parents or carers who have children attending the School.

Schools have a key role to teach young people about the importance of how to communicate safely and respectfully online, keeping personal information private.

- Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

Concerns regarding children's use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

11. Mobile Devices (Including Bring You Own Device-BYOD)

Mobile devices refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras and digital watches.

Bring your own device—also called bring your own technology, bring your own phone, and bring your own personal computer—refers to the policy of permitting employees to bring personally owned devices to their workplace, and to use those devices to access privileged company information and applications.

A policy which prohibits users from taking mobile devices to school is unreasonable and unrealistic for schools to achieve. St Mary's School has adopted a policy that:

- Mobile phones shall not be used on the School premises. Signs are displayed around buildings to that effect. The one exception is the mobile phone used by the After-School Club to manage attendance and pick-up arrangements.

- Mobile devices may be used during lessons or formal school time as part of approved and directed curriculum-based activity.

- Mobile devices brought in to School remain the responsibility of the owner. The School accepts no responsibility for the loss, theft or damage of such items.

- School staff authorised by the Headteacher may search pupils or their possessions, and confiscate any mobile device they believe is being used to contravene School policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.

- Where staff need to contact parents within or outside of the School setting in a professional capacity, they should only do so via an approved School account (email, telephone, social media). In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP.

- Staff will be provided with School equipment for the taking of photos or videos of pupils linked to an educational intention. In exceptional circumstances, staff may need to use personal devices for such a purpose and when doing so, should ensure they comply with the school's Responsible Internet Use Agreement.

- Users are to connect mobile devices through the School's wireless provision that allows the ability to filter any device that uses the School Internet connection.

- The School will take steps to monitor responsible use in accordance with the Responsible Internet Use guidelines.

12. Video-Conferencing

Video-conferencing (including FaceTime, Skype and Lync), enables users to see and hear each other between different locations.

- This real time interactive technology should take place using the School's wireless system.
- Staff must refer to any Responsible Internet Use agreements prior to children taking part in video conferences.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Video conferencing will be supervised appropriately for the pupil's age and ability.

13. Cyber Bullying

Cyber bullying is defined as the use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone (DCSF2007). It is essential that young people, school staff, parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Pupils, staff and parents/carers are required to work with the School to support its approach to cyber bullying and the School's e-Safety ethos.

Cyber bullying, as with all other forms of bullying, of or by any member of the School community will not be tolerated. Full details are set out in the School's Behaviour, Anti-bullying and Safeguarding & Child Protection policies.

Implementation

14. Policy in Practice - Staff

- The E-Safety Policy will be provided to and discussed with all members of staff. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they are to discuss this with their senior leader to avoid any possible misunderstanding.
- Staff should be aware that Internet traffic is monitored and automatically reported by the ISP and can be traced to the individual user.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff must be made aware of their responsibility to maintain confidentiality of school information.
- All members of staff will be made 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 bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

15. Policy in Practice - Parents

- Internet issues will be handled sensitively to inform parents without undue alarm.
- Regular information will be provided to parents about how to ensure they can work with the School to ensure this resource is used appropriately both within school and home.
- Parents will be made aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk.
- Parents' attention will be drawn to the Responsible Internet Use guidelines in newsletters, School prospectus and School website. Relevant websites are listed in the Links section of the School website for easy access.

- A partnership approach with parents will be encouraged. This includes offering parent meetings, demonstrations, practical sessions and suggestions for resources and safer Internet use at home.

16. Handling of complaints

Parents and staff must know how and where to report e-safety-related incidents in line with the School's Complaints policy and Safeguarding & Child Protection Policy.

END

Appendix A

Dear Parents / Carers

Responsible Internet Use

As part of your child's curriculum and their development of computing skills, St Mary's Catholic Primary School provides supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children.

Please read the attached Rules for Responsible Internet Use so that your child may use the Internet at School.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our School Internet provider, Oakford Technology, operates a filtering system that restricts access to inappropriate materials. This may not be the case at home, please see our School website for information regarding internet safety.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use, or would rather your child did not access the internet, please inform me in writing.

Yours sincerely

Headteacher

St Mary's Catholic Primary School

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- **I will ask permission before using the Internet.**
- **I will use only my own class network login and password.**
- **I will only look at or delete my own files**
- **I will only look at or delete other people's files with permission from a member of staff.**
- **I understand that I must not bring software or disks into school without permission.**
- **I will only e-mail people my teacher has approved.**
- **The messages I send will be polite and sensible.**
- **I understand that I must never give my home address or phone number, or arrange to meet someone.**
- **I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.**
- **If I see anything that I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.**
- **I understand that the School may check my computer files and the Internet sites I visit.**
- **I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.**

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

Appendix B

Responsible Internet Use Consent Form Please complete, sign and return to the School Office	
Pupil:	
Pupil's Agreement I have read, and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way, and obey these rules at all times.	
Signed:	***Date:***
Print Name:	
Parent's Consent for Web Publication of <u>Work</u> I agree that, if selected, my son/daughter's work may be published on the School website.	
Signed:	***Date:***
Print Name:	
Parent's Consent for Web Publication of <u>Photographs/videos</u> I agree that, if selected, my son/daughter's photograph may be published on the School website, School Facebook account and/or the School's Twitter feed (please indicate YES/NO below for each aspect). Please note: names will never be used to identify a child in a photograph/video.	
Signed:	***Date:***
Print Name:	

Website – http://www.st-marys-pri.wilts.sch.uk/	
Facebook –	
Twitter -	

Parents are permitted to take photographs at School events where their child is the focus of the photograph. Whilst it is parental choice as to whether they post photographs of their own children on social media, parents are asked not to post photographs where other children can be identified without the permission of the parents of the children concerned.

If there are any concerns expressed by parents with regards to photographs of their children being posted against their wishes the School will review the situation and may need to request that photographs are not taken in the future.