



St. Joseph's Catholic Primary School

Digital Safety Policy

Statement of Intent

St Joseph's Catholic Primary School has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff. We as a school are committed to providing a safe learning and teaching environment for all pupils and staff, and have implemented important controls to prevent any harmful risks.

At St Joseph's, we understand that the internet is regarded as an essential resource to support teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives. Young people have access to the internet from many places - home, school, friends' homes, libraries and in some cases, mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn how to be safe when online. We also believe that schools should strive to support parents in understanding the issues and risks associated with children's use of digital technologies by making our parents aware of the procedures for online safety within the school through our policy.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an internet environment as possible and a need to teach them to be aware of, and respond responsibly to, the risks.

Core Principles of Internet Safety

The internet is becoming as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations.

Our Online Safety Policy is built on the following five core principles:

Guided educational use

Significant educational benefits should result from curriculum internet use including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful internet use will also reduce the opportunities for activities of dubious worth.

Risk assessment

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become 'internet wise'. Pupils need to know how to cope if they come across inappropriate material.

Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves, taking responsibility for the use of internet and other communication technologies such as mobile phones. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully. There are a number of technical solutions to help limit internet access, although it is the appropriateness and consistency of the school's e-safety policy that is of overriding importance.

Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied. For instance, unmoderated chat rooms present immediate dangers and are banned. Fair rules, clarified by discussion and prominently displayed at the point of access help pupils make responsible decisions.

Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

Why is Internet use important?

- 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 use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century 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.

How does the Internet benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and,
- exchange of curriculum and administration data with the LA and DfES.

How will Internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will learn appropriate Internet use, what is and what is not appropriate use, and given clear objectives for Internet use.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

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 will be sought at the start of each Key Stage. Oakford Technologies Ltd proactively monitors internet usage for illegal (attempted access of child abuse and incitement for racial hatred) websites and will notify the local police and Local Authority in these instances.

- Primary pupils will not be issued individual email accounts, but will be authorised to use a group/class email address under supervision.
- Parents will be asked to sign an agreement that will include the acceptable use policy and guidance for video, sound and images for web publication.
- The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date; for instance a member of staff may leave or a pupil's access be withdrawn.
- 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.

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 the school community from youngest pupil to staff. Wiltshire LA, in conjunction with the Internet Watch Foundation (IWF) has implemented Netsweeper.

This service filters internet access by cross-referencing all website requests against a banned list which is continually updated.

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the internet Service Provider Oakford Technologies Ltd via the Computing Lead.
- The school will work in partnership with parents; Wiltshire County Council, DCFS and the Internet Watch Foundation (IWF) to ensure systems to protect pupils are reviewed and improved.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Historical reports of internet usage are sent on a monthly basis to admin@st-josephs-malmesbury.wilts.sch.uk for monitoring.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (IWF).

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.

- 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 County 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.

Managing Content

How will pupils learn to evaluate internet content?

Pupils need to understand that some content is deliberately misleading, while some is/may be unsuitable from purely a reading age perspective. Ideally, inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering.

Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the URL to the teacher for inclusion in the list of blocked sites. More often, pupils will be judging reasonable material but need to select that which is relevant to their needs, for instance to answer a question. Pupils should be taught research techniques and encouraged to question the validity, currency and origins of information – looking for the author's name, date of revision and whether there are other links to the site. Pupils should also use alternative sources of information for comparison purposes. Effective, guided use should also reduce the opportunity pupils have for exploring undesirable areas.

Access to sensitive sites, for example those that record the Holocaust, may be required for the duration of a specific educational activity by supervised pupils of appropriate age. The school has the ability to permit and deny websites and specific content through our own local filtering. Using internet derived materials in pupils' own work requires at least an understanding that straight copying is worth little without a commentary that demonstrates the selectivity used and evaluates significance.

Respect for copyright and intellectual property rights, and the correct usage of published material needs to be taught.

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to Oakford Technologies Ltd: 01380 888088 or email the computing lead rachel@st-josephs-malmesbury.wilts.sch.uk
- Schools should ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Specific lessons will be included within the Computing Scheme of Work that teaches all pupils how to read for information from web resources.
- The Head teacher will be responsible for permitting and denying additional websites as requested by colleagues.

How should website content be managed?

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Communication

Managing e-mail

Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires that the implications for the school and for the pupils have been thought out and that appropriate safety measures have been put in place.

- Pupils will only have access to their own individual email through the safe forum of Purple Mash. This means that they are only able to email to the school community.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Pupils should use email in an acceptable way. Sending images without consent or messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.
- Access in school to external personal e-mail accounts is blocked.
- 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.

On-line communications and social networking.

All of these services are filtered by Oakford Technologies Ltd. These are banned from pupil access while at school, but are likely to be accessible from home. Schools have a key role to teach young people about the importance of keeping personal information safe, not posting comments and pictures of other people that may cause upset and to communicate in an appropriate manner.

- Students/pupils will be taught about how to keep personal information safe when using online services. Each year group will have specific computing lessons dedicated to e-safety.
- The use of online chat is not permitted in school.

Mobile technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones are not permitted for children in school.

Introducing the Policy to Pupils

- Rules for internet access will be posted in all rooms where computers are used.
- A module on responsible internet use and online safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.
- Instruction on responsible and safe use should precede internet access.
- Pupils will be informed that internet use will be monitored.
- All Key Stage 2 pupils will use the online safety activities from the Wiltshire primary schools ICT Scheme of Work to help teach internet Safety

Parents and Online Safety

- Parents' attention will be drawn to the School Digital Safety Policy in newsletters, the school brochure and on the school Website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- 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.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children.
- All parents will receive support information as and when available.
- The school takes no responsibility for the security of pupils carrying out school based activities on home computers.
- Interested parents will be referred to organisations such as Child Exploitation and Online Protection (CEOP).
- All parents will be required to agree to the Responsible Internet Use rules for their children and sign a consent form for their child to have Internet access at school.

Consulting with Staff and their inclusion in the Digital Safety Policy

All school staff need to be aware that they are subject to the same conditions as any Wiltshire County Council employee on internet misuse. Clearly checking a website for a holiday weather forecast is unlikely to be an issue, but the use of a school email address to send racist jokes could be grounds for misconduct.

Internet use is widespread and all staff including administration, governors and helpers should be included in appropriate awareness-raising and training. Any groups using the school's ICT facilities and in particular the internet should sign a copy of the acceptable use policy before being provided with access. Internet use should be included in the induction of new staff.

- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Digital Policy, and its importance explained.
- The school's consequences for internet misuse will be clear so that all teachers are confident to apply this should the situation arise.
- All staff must accept the terms of the 'Responsible internet Use' statement before using any internet resource in school.
- Staff should be aware that internet traffic is monitored and reported Oakford Technologies Ltd and can be traced to the individual user. Discretion and professional conduct is essential.
- Community users of the school's ICT facilities must sign the acceptable user policy before being granted access.
- Staff development in safe and responsible internet use and on the school internet policy will be provided as required.

How will complaints be handled?

Parents and teachers must know how and where to report incidents. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. All record of the incident should be kept e.g. e-mails saved or printed, text messages saved etc. Complaints of a child protection nature must be dealt with in accordance with the LA Child Protection procedures.

- Responsibility for handling incidents will be delegated to the Head teacher.
- Any complaint about staff misuse must be referred to the Head teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Signed: (Head teacher)

..... (Chair of Governors)

Reviewed:

Review:

Laptop policy for St. Joseph's school staff

1. The laptop remains the property of St. Joseph's School.
2. The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only St. Joseph's School Staff should use the laptop.
3. On the teacher leaving the school's employment, the laptop is returned to St. Joseph's School. Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the Head teacher).
4. Whenever possible, the laptop must not be left in an unattended car. If there is a need to do so it should be locked in the boot.
5. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the Head teacher with evidence of adequate insurance.
6. Staff may load their own software onto the laptop but it must be fully licensed and not corrupt any software or systems already installed on the laptop.
7. Any software loaded must not affect the integrity of the school network.
8. If any removable media is used then it must be checked to ensure it is free from any viruses.
9. It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop is kept up to date.
10. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
11. Students must never use the laptop.
12. If any fault occurs with the laptop, it should be reported to Oakford immediately.
13. The laptop would be covered by normal household insurance. If not it should be kept in school.

Online Safety: Staff, Governors and Volunteers Responsible Use Agreement

This Responsible Use Agreement is part of the school's Online Safety Policy and must therefore be adhered to at all times. The agreement is intended to ensure that:

- All staff, governors and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.
- The school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff, governors and volunteers are protected from potential risk in their use of computing in their everyday work.

Responsible Use Agreement

I understand that I must use school computing systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor the use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the e-safety co-ordinator.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will not delete any resources produced for whole department use unless they have been updated.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video

images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will not use social networking sites in school.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner. I will not give students my personal email address.
- I will only give students my personal mobile phone number if authorised (for example on a school trip) and will tell students to delete any staff numbers once they are no longer needed.
- I will not contact any students via a social networking site and will ensure that there is nothing inappropriate on the public profile of my social networking site.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (tablets/laptops/mobile phones/USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes. I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on any machine, or store programmes on a computer, nor will I try to alter computer settings without the permission of the Network Manager.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will encrypt any data that is determined to be personal or sensitive in nature if transporting it (e.g. on a USB stick).
- I will not store any data which includes details of students on any personal devices.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Responsible Use Policy, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

Name:.....

Signature:

Date:



St. Joseph's Catholic Primary School

Acceptable Use of Technology Agreement: EYFS and KS1

Our school recognises the important contribution and value technology can play in promoting your learning and development, however, there are potential risks involved. We have a rigorous online safety policy in place, alongside procedures to keep your child safe. Both the staff recognise online safety issues and plan carefully to make sure that you can use the internet safely.

We want to help your child stay safe whilst developing a considerate, appropriate and responsible approach to using the internet. Their understanding of the potential dangers must develop as their online independence grows with age.

The following agreement is designed to help your child understand their responsibilities when online in school (either using the internet or our school network) and at home. In KS2, it is expected that your child will have a strong enough understanding to sign this document themselves. However, in EYFS and KS1, parents are required to sign it on their behalf. Each class will go through the agreement on a regular basis. Despite this, it is important to talk through the agreement (or those that apply to your child's understanding) before signing.

This is how we stay safe when we use computers:

- I will ask a teacher or teaching assistant if I want to use the computers / tablets.
- I will only use activities that a teacher or teaching assistant has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or teaching assistant if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or teaching assistant if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer / tablet.
- I will not share personal information about myself with people I don't know on line.

Pupil Acceptable Use Agreement Form

St. Joseph's Catholic Primary School Acceptable Use of Technology Agreement for EYFS & KS1 children and parents <i>Please complete, sign on the behalf of your child and return to the school</i>	
<i>Please print name:</i>	
Parent's Consent for Internet Access I have read and understood the school rules for Acceptable Use of Technology agreement and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.	
Signed:	Date:



St. Joseph's Catholic Primary School

Acceptable Use of Technology Agreement: KS2

Our school recognises the important contribution and value technology can play in promoting your learning and development, however, there are potential risks involved. We have a rigorous online safety policy in place, alongside procedures to keep your child safe. Both the staff recognise online safety issues and plan carefully to make sure that you can use the internet safely.

We want to help your child stay safe whilst developing a considerate, appropriate and responsible approach to using the internet. Their understanding of the potential dangers must develop as their online independence grows with age.

The following rules are designed to help your child do this when online in school (either using the internet or our school network) and at home. At KS2, it is expected that your child will have a strong enough understanding to sign this document themselves. However, at KS1, parents are required to sign it on their behalf. Each class will go through the rules on a regular basis. Despite this, it is important to talk through the rules (or those that apply to your child's understanding) before signing.

Rules for Responsible Internet Use

- I will always ask before using computers in school.
- I will only use the internet in school for learning purposes.
- I will always ask an adult in school before using the internet.
- I will use only my personal login and password, which is secret.
- I will always be kind and respectful to other users when online.
- I will only open my own files and ask a teacher before deleting anything.
- I will only use photographic devices (webcam, digital camera, iPad etc.) to take photographs with my teacher's permission.
- I will only download materials from the internet with my teacher's permission, storing them in an agreed folder.
- I understand that social networking should only be used outside school with my parents' permission.
- I must ask an adult before using any external hardware (memory sticks, CDs etc).
- I will only e-mail and open attachments that my teacher has approved.
- The messages I send will be polite and sensible.

- I will keep my personal information safe.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell an adult immediately.
- I understand that the school may check my computer files, e-mails I send 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 for specific amount of time, decided by my teacher.
- I understand that, for my safety, the school is allowed to monitor my internet activity, including emails and the websites that I look at.
- I know that the South West Grid for Learning (SWGfL) monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.
- I understand the importance of appropriately acknowledging the ownership of material found on the internet before copying, downloading or using it.
- **Year 6 only** – If bringing a mobile phone into school it must be handed to the teacher at the start day.

St. Joseph's Catholic Primary School Acceptable Use of Technology Agreement for KS2 children and parents Please complete, sign and return to the school	
Pupil:	Class:
Pupil's Agreement I have read and I understand the school rules for Acceptable Use of Technology agreement. I will use the computer system and Internet in a responsible way and follow these rules at all times.	
Signed:	Date:
Parent's Consent for Internet Access I have read and understood the school rules for Acceptable Use of Technology agreement and give permission for my son / daughter to access the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.	
Signed:	Date:
Parent's Consent for Web Publication of Work and Photographs I agree that, if selected, my son/daughter's work may be published on the school website. I also agree that images, sound files and video that include my son/daughter may be published subject to the school rules that this content will not clearly identify individuals and that full names will not be used.	
Signed:	Date: