ST. JOHN'S CATHOLIC PRIMARY SCHOOL

Online Policy

March 2026

Our Mission Statement

The Mission of St. John's Catholic Primary School is to grow and learn in the footsteps ofJesus by being: responsible, caring, prayerful, creative, independent, thoughtful, curious and respectful. We live our Mission by:

- Ensuring that our attitudes and values are transmitted through a curriculum that isconsistent with the Catholic faith
- Delivering a curriculum that is relevant, varied, interesting, stimulating, balanced andappropriate
- Developing policies and schemes of work which recognise that R.E. is an integral part ofthe curriculum
- Developing sound teaching and effective classroom management
- Generating a positive attitude to learning where realistic expectations of pupils and highstandards of work are expected
- Using a variety of teaching approaches that reflect the needs of individual pupils
- Participating in projects which focus on the needs of others including local and international charities.
- St. John's is a Catholic voluntary aided primary school, established by the Church to serve the parishes of St. John the Baptist, Trowbridge, St. Bernadette's, Westbury and St. Thomas Moore, Bradford on Avon.

1. Introduction

The Internet is now regarded as 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. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

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 notusually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe.

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 tobe aware of and respond responsibly to the risks.

2. 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 of pupils in embarrassing, inappropriate and even dangerous situations. Schools need a policyto help to ensure responsible use and the safety of pupils.

St. John's Catholic's Online Policy is built on the following five core principles:

2.1 Guided educational use

Significant educational benefits should result from curriculum Internet use including access to information from around the world and the abilities 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.

2.2 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". Schools need to ensure thatthey are fully aware of the risks, perform risk assessments and implement a policy for Internet use. Pupils need to know how to cope if they come across inappropriate material.

Pupils may obtain Internet access in youth clubs, libraries, and public access points and inhomes. Ideally a similar approach to risk assessment and Internet safety would be taken inall these locations, although risks do vary with the situation.

2.3 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, though; it is the appropriateness and consistency of the school's e-safety policythat is of overriding importance.

2.4 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 un-moderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will helppupils make responsible decisions.

2.5 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. Strategies must be selected to suit the school situation and their effectiveness monitored. There are no straightforward or totally effective solutions and staff,parents and the pupils themselves must remain vigilant.

3. Who will write and review the policy?

This online policy has been written and adapted by the school, building on the Wiltshire e-safety template and government guidance. It has been agreed by the senior management and approved by governors and it will be reviewed annually. The policy will be written with regard to GDPR and should be read in conjunction with the schools Privacy policy.

4. Why is Internet use important?

The purpose of Internet use in school is to;

- Raise educational standards,
- Promote pupil achievement and well being
- Support the professional work of staff
- 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 pupils 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 pupils with quality Internet access as part of their learning experience.

5. How will Internet use enhance learning?

The school Internet access will be designed expressly for educational use and will include:

- Filtering appropriate to the age of pupils.
- Pupils will learn appropriate Internet use and be given clear objectives for Internet use.
- Staff should guide pupils in online activities that will support the learning outcomesplanned for the pupils' age and maturity.

6. How will Internet access be authorised?

- 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'saccess be withdrawn.
- Our pupils' home-school agreement will include the acceptable use policy and guidance
- For video, sound and images for web publication. (See Appendix).
- Our pupils can be issued with individual email accounts, but this will be authorised andused under supervision and to addresses within the school network.

7. How will filtering be managed?

- The schools IT supplier will review the popular permitted and banned sites accessed by the school, and report to the designated governor at least twice a year.
- The school will work in partnership with parents, Wiltshire Council, DCSF, the schoolData Protection Officer, and Oakford Technology to ensure systems to protect pupilsare reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider (Oakford Technology) via the Computing Subject Leader.
- Any material that the school believes is illegal must be referred to the Internet Watch.

8. How will the risks be assessed?

- 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 global 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 couldconstitute 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 andcompliance with the policy monitored.

9. Managing Content

9.1 How will pupils learn to evaluate Internet content?

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to Oakford Technology

- The school will ensure that the use of Internet derived materials by staff and by pupilscomplies with copyright law.
- Specific lessons will be included within the Computing Scheme of Work that teachesall pupils how to read for information from web resources.
- A nominated person, from the SLT or the schools IT supplier, will be responsible for permitting and denying additional websites as requested by colleagues.

9.2 How should the school's 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.
- Photographs for parts of School Website and Virtual Learning Environment (VLE) thatinclude pupils will be selected carefully. Photographs on the public facing websites willnot enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the public facing parts of the School Website or VLE.
- The Website will comply with the school's guidelines for publications.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the School Website, VLE or written publications for the school,and this permission can be withdrawn at any time. This will usually be done at the beginning of the first school year and kept on file.
- Pupils and parents have the responsibility to comply with school rules and proceduresin regard to e-safety of all persons.
- The copyright of all material will be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

10. Communication

- Pupils may only use approved e-mail accounts (where applicable) on the school system.
- 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, suchas address or telephone number, or arrange to meet anyone.
- Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.

10.1 On-line communications and social networking

- Pupils will be taught about how to keep personal information safe when using onlineservices.
- Pupils are taught how to communicate appropriately online through the Teach Computing scheme.
- The use of online chat rooms is not permitted in school, other than as part of its onlinelearning environment.
- The use of Social Media for example Facebook, Twitter must not be accessed.

10.2 Mobile technologies

- Emerging technologies will be examined for educational benefit and a risk assessmentwill be carried out before use in school is allowed.
- Mobile phones **are not permitted** within the school. Pupils will be asked to give themto the school office at the start of the school day. Any parent needing to contact their

child(ren) can contact the school on tel: 01225 752006. The school will contactparent/carer as necessary via telephone on behalf of the child(ren) where appropriate.

11. Introducing the Policy to Pupils

- Pupils are taught how to act responsible when using the internet through the Teach Computing scheme, Internet Safety day and external companies e.g. Stay Safe Initiative.
- Instruction on responsible and safe use should precede Internet access.
- Pupils will be informed that Internet use will be monitored.

12. Parents and Online Safety

- Parents' attention will be drawn to the School Online Safety Policy in newsletters.
- The Online Safety Policy will be published on the School Website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged.
- Parents are asked to show discretion when uploading images or videos to social media taken of their own children at school or school events and to ensure they do not include other identifiable children from St John's unless they have obtained permission from their parents /carers.

13. Governors and Online Safety

- Governors are reminded to only use their allocated school email addresses when communicating with the school.
- If the content of emails is sufficiently sensitive then attachments should be passwordprotected. (such as when a specific child or teacher could be identified)
- Governors are to ensure they are familiar with the issues surrounding GDPR and abide by the schools policies at all times.
- Upon completion of their term of office all school related documents should be deletedfrom their personal computers / tablets etc. and paperwork either destroyed at home or handed back to school for shredding.
- Care must be taken when accessing school data remotely in public places that confidential or sensitive information is not visible by members of the public thereby compromising the integrity of information.

14. Consulting with Staff and their inclusion in the Online Safety Policy

- All staff including teachers, classroom assistants and support staff, will be provided with the School E-Safety Policy, and its importance explained.
- The school's consequences for Internet and mobile phone / tablets / technology misuse will be clear so that all teachers are confident to apply this should the situationarise.
- 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 by Oakford Technology and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

15. How will complaints be handled?

- Responsibility for handling incidents will be delegated to a senior member of staff.
- 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.

Responsible Internet Use
for all children

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

- I will ask permission to use an iPad/laptop/chrome book
- I will ask permission before using the Internet.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission.
- I will only e-mail and open attachments that I was expecting, from people I know, or my teacher has approved. If emails do not look and feel right I will not open any attachments or click any links – and I will speak to my teacher.
- The messages I send will be polite and sensible.
- I will ask permission before I post.
- I will not post or copy anyone's image without permission.
- I understand that I must never give my home address or phone number, or arrange tomeet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell ateacher immediately.
- I understand that the school may check my computer files, e-mails I send and theInternet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use theInternet or computers for an agreed period of time
- I understand my password is secret to me, and I will not share it

The school may 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 betaking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

St. John's Catholic Primary School

Dear Parents,

Responsible Internet and Device Use

As part of your child's curriculum and the development of computing skills, St. John'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 as they grow up in the modern world. Please would you read the attached **Responsible Internet Use poster** and sign and return the consent form so that your childmay use the Internet and electronic devices at school.

Our school Internet provider, Oakford Technology, operates a filtering system that restrictsaccess to inappropriate materials. In addition staff, pupils and parents are all expected to report inappropriate content immediately. 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 Internetfacilities.

Should you wish to discuss any aspect of Internet use please telephone me to arrange anappointment.

Yours sincerely

Mrs K O'Rourke

Head Teacher

Responsible Internet Use Consent Form

Please complete, sign and return to the school office

Pupil:	Class:

Pupil's Agreement

I have read and I understand the school Rules for Responsible Internet and VLE use.
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 and electronic device usage

I have read and understood the school rules for responsible Internet and VLE use 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 & educate on how to respond effectively if they encounter inappropriate materials. I understand that the school cannot be held responsible for the nature orcontent of materials accessed through the Internet. I agree that the school is not liable for any damages
arising from use of the Internet.

Signed:	Date:

Please print name:	

Parent's Consent for Web Publication of Work andPhotographs

I agree that, if selected, my son/daughter's work may be published on the School's Public Facing Website& school social media accounts. I also agree that images, sound files and video that include my son/daughter may be published subject to the school rules that the supporting text will not clearly identify
individuals and that full names will not be used. I understand I can withdraw consent at any point bycontacting the school office.

Signed:	Date:

Please print name:	

Learner Acceptable Use Agreement Template – for KS2

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.
This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.
For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that adults have told me are safe to visit
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of "stranger danger" when I am online
- I will not share personal information about myself or others when online
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do
- I will think about how my behaviour online might affect other people:
- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will not use my own personal device in school (mobile phones/USB devices etc.)
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

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

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, there will be consequences.

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.
I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: ..... Class:.....

Signed:..... Date:……..

Parent/Carer Countersignature

Name…….

Signed …….. Date……

16. Staff Policy for St. John's Catholic school

(a) Devices (e.g. laptops / tablets)

1. The device remains the property of St. John's Catholic School.
2. The device is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility remains with the teacherallocated. Only St. John's Catholic School Staff will use the device.
3. On the teacher leaving the school's employment, the device is returned to St. John's Catholic School.
4. Staff on extended leave of 4 weeks and over should return their device to the school (other than by prior agreement with the head teacher).
5. Whenever possible, the device must not be left in an unattended car. If there is a needto do so it should be locked in the boot, but only as a temporary measure (e.g. stoppingoff on the way home)
6. The device 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 adequateinsurance.
7. All programmes and software require licenses and should only be installed by Oakford Technology.
8. If any removable media is used then it must be checked by the technician to ensure itis free from any viruses prior to use, and must not be used to store personal data (e.g.pupil data), unless it is encrypted. Likewise any use of a memory stick must be a temporary one, and the data should be uploaded to the school network as soon as possible and removed from the external memory afterwards.
9. Staff must use their device in school and on the school network at least once a week(term time) to ensure virus protection is automatically updated.
10. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
11. Pupils must never use the allocated device unless supervised.
12. If any fault occurs with the device, it should be referred immediately to the technicianvia the helpdesk.

(b) Responsible e-mail, network and Internet use

1. I will use all ICT equipment issued to me in an appropriate way. I will not:

    - Access offensive websites or download offensive material.
    - Make excessive personal use of the Internet or e-mail.
    - Copy information from the Internet that is copyright or without the owner'spermission.
    - Place inappropriate material onto the Internet.
    - Will not send e-mails that are offensive or otherwise inappropriate.
    - Disregard my responsibilities for security and confidentiality.
    - Download files that will adversely affect the security of the device and school network.
    - Access the files of others or attempt to alter the computer settings unless explicitlyasked to do so such as when sharing files stored in the cloud. (e.g. Google Drive /Sharepoint)
    - Update web pages etc. or use pictures or text that can identify the school, without the permission of the head teacher. When I use photos or footage of pupils I will check the necessary consents are in place.

- Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of St. John's Catholic School.

2. I will only access the system with my own name and registered password, which I willkeep secure, using a school device.
3. I will inform the School's Technician as soon as possible if I know my password is nolonger secure
4. I will always log off the system when I have finished working, and will lock my device when away from it (using Ctrl-Alt-Del or + L)
5. I understand that the school may, in line with this policy, check my computer files andemails and may monitor the Internet sites I visit.
6. My files should not, routinely, be password protected by my own passwords. Shoulda confidential matter warrant this, I must gain permission from the head teacher and register the passwords with the head teacher, or use access permissions within the school network to protect access to the data.
7. When working on school data on a device in a public environment (e.g. public transport, coffee shop) I will ensure my screen is protected from those who should notaccess school data (a Privacy Screen will assist with this).
8. Any work I undertake using cloud services (such as Google Drive) will be securely protected by passwords and not shared with people not connected with the school. I will ensure they are not made public but only shared with specific named individuals.
9. If I use removable media, I will ensure that this has been carefully checked to ensureit is free from any type of virus, and must not be used to store personal data (e.g. pupildata), unless it is encrypted Likewise any use of a memory stick must be a temporaryone, and the data should be uploaded to the school network as soon as possible, andremoved from the external memory stick afterwards.
10. I will not open e-mail attachments, or click links in emails if they do not look and feel right, If I am unsure I will check with the sender by other trusted means (e.g. phone call, SMS)
11. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used and will not be copied to other staff or contacts.
12. When emailing multiple external recipients, I will use blind copy (BCC) so that all the email addresses are not disclosed to one another, and will check the accuracy of the email address from the primary information system (e.g. SIMS).
13. I will report immediately to the head teacher any unpleasant material or messages sent to me.
14. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
15. Use of any part of the school IT system, portals or services owned or purchased by the School for personal financial gain, gambling, political purposes or advertising is forbidden.
16. Storage of e-mails and attachment should be kept to a minimum to avoid unnecessarydrain on memory and capacity.
17. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
18. When using my own device (e.g. personal phone, laptop, tablet) to access school emails I will ensure that
    - The device is secured with a PIN, Password or fingerprint
    - The device has anti-virus installed
    - The device has the latest updates applied
    - I log out of all applications after use, and not use the save my password function
    - I do not save/download any data to the local device (e.g. email attachments)

19. I understand that by adding School email account to my personal device I enable theSchool to remotely delete information on my personal device.
20. I understand that if I do not adhere to these rules, my network access may be suspended immediately, my device removed and that other disciplinary consequences may follow.

Name.....

Signature: .....

Date: .....

18. Web-based ResourcesFor

Schools

KidSmart http://www.kidsmart.org.uk/

SMART rules from Childnet International and Know It All for Parents

Childnet International http://www.childnet-int.org/

Guidance for parents, schools and pupils

Becta / Grid Club, Internet Proficiency Scheme

On-line activities for Key Stage 2 pupils to teach e-safety.

http://www.gridclub.com/teachers/t_internet_safety.html

Kent Local Authority http://www.clusterweb.org.uk/kcn/e-safety_home.cfm

Additional e-safety materials (posters, guidance etc.)

London Grid for Learning http://www.lgfl.net/lgfl/sections/safety/esafety/menu/

Additional e-safety materials (posters, guidance etc.)

DfES Anti-Bullying Advice http://www.dfes.gov.uk/bullying/

Internet Watch Foundation www.iwf.org.uk

Invites users to report illegal Websites

South West Grid for Learning – Safe www.swgfl.org.uk/safe

A comprehensive overview of web-based resources to support schools, parents and pupils

Think U Know? www.thinkuknow.co.uk/

Home Office site for pupils and parents explaining Internet dangers and how to stay incontrol.

Wiltshire County Council – WISENET Child

protection advice relating to e-safety

National Online Safety www.nationalonlinesafety.com

Providing resources for schools

For Parents

Kids Smart http://www.kidsmart.org.uk/parents/advice.aspxA

downloadable PowerPoint presentation for parents

Childnet International http://www.childnet-int.org/

"Know It All" CD-ROM free to order resource for parents to help raise awareness of how tohelp their children stay safe online.

Common Sense Media www.commonsensemedia.org

Reviews and age ratings for apps and films

CEOP www.ceop.police.uk

Child Exploitation and Online Protection Centre

This policy should be read in conjunction with the child protection and safeguarding policy.

This policy has been approved and adopted by the Governing Body.

Headteacher: Mrs K O'Rourke

Chair of Governor: Mrs C Doogue

Review cycle:	Annually
Next review due:	March 2027