Saint Patrick's Catholic Primary School

Our Mission in Saint Patrick's is to develop each child's talents potential in a caring Catholic community inspired by the teachings of Jesus Christ.

SAFEGUARDING – Keeping ALL of Our Children Safe

ONLINE SAFETY POLICY
2025/2026

Saint Patrick's Catholic Primary School fully recognises its responsibilities for child protection.

RATIONALE

The Internet is regarded as an essential resource to support teaching and learning. The statutory national 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, such as phones. Computer skills are vital to access life-long learning and employment; indeed, ICT is now seen as an essential life-skill, following the pandemic 2020 onwards.

In line with school policies that protect pupils from other dangers (see Safeguarding suite of policies on school website), 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.

This policy should be read alongside the following other school policies:

* Anti Bullying Policy * Behaviour and Self-Regulation Policy * Child Protection Policy * Evolve documentation * Equality Policy * GDPR Statement * Health and Safety Policy * Home School Agreement * Intimate Care Policy * Medical Needs and Administering Medicine Policy * Mission Statement * Safer Recruitment Policy * Staff Behaviour Policy * Whistleblowing Policy

In addition all staff will have read and understood Part 1 of the latest version of *Keeping Children Safe in Education*, (KCSiE), September 2025. This now focusses specifically on online safety, with content being added and strengthened to ensure online safety is clearly viewed as part of a school's statutory safeguarding responsibilities.

The technologies children and young people are accessing are constantly developing and changing. As a staff it is essential to develop our understanding of the technologies that children and young people are able to access. This includes a variety of internet learning aids available both in and out of the classroom.

There are many benefits to using internet-based learning aids; however, these websites are not always policed and content needs to be carefully reviewed. All users need to be aware of the risks associated with using these technologies.

At St Patrick's Catholic Primary School Primary School, we understand the responsibility to educate our pupils on Online Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. 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 administration systems. It is important that all users of the internet at our school are aware of the risk of misinformation, disinformation and conspiracy theories as set out in KCSIE 2025.

Following the reviews to KCSiE 2025, all staff have continued to be provided with online safety information and training at induction, and have received updated online safety training as part of their annual child protection training. Children are taught about online safety at the appropriate level of understanding for their age and a more personalised or contextualised approach is put in place for more vulnerable children e.g. victims of abuse

and SEND. Parents also receive updated Online Safety information through a workshop in Autumn 2025, which can be found in video guidance on the class Tapestry and Google Classroom pages.

SCHOOL PROCEDURE AND PRACTICE IN ONLINE SAFETY

1. ROLES AND RESPONSIBILITIES

As Online Safety is an important aspect of strategic leadership within the school the Governing Body has ultimate responsibility to ensure that the policy and practices are embedded and monitored. This responsibility is delegated to the Headteacher. Any extra permission given by the Headteacher must be recorded (e.g. memos, minutes from meetings) in order to be valid.

The Designated Senior Leader for Child Protection (J. Courtney), the Deputy DSLs (C. Sykes/C. Minty) and Computing Subject leader (C.Minty) have the responsibility of ensuring this policy is upheld by all members of the school community and that they have been made aware of the implication this has. It is the responsibility for these members of staff to keep practice up to date through training and current issues. All members of staff must be made aware of any new information regarding Online Safety.

2. ONLINE SAFETY SKILLS DEVELOPMENT FOR ALL STAFF

- Our staff receive regular information and training on Online Safety issues in the form of full staff meetings and memos.
- Online Safety updates are shared with staff when received from Wiltshire LA or National Guidance
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate Online Safety activities and awareness within different curriculum areas.

3. COMMUNICATING THE SCHOOL ONLINE SAFETY MESSAGE

- Online Safety rules will be discussed and developed with the pupils throughout the year as part of the Computing Curriculum.
- Visits and assemblies from those in positions of authority (i.e. local Police officers) will take place during the year, especially with regards to social media and appropriate uses of technologies.
- Pupils will be informed that network and Internet use will be monitored.
- Online Safety posters will be prominently displayed throughout the school.
- Parents will be given opportunities to develop their understanding of how to promote Online Safety at home through information in school newsletters and information in the Online Safety Videos on each classes Tapestry of Google Classroom pages. We hold a specific Online Safety Guidance meeting ahead of each 'Meet the Teacher' event in the Autumn term. Information is also on the school website.

4. ONLINE SAFETY IN THE CURRICULUM

ICT and online resources are increasingly used across the curriculum. At Saint Patrick's Catholic Primary, we believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote Online Safety. We regularly discuss and monitor our pupils' understanding of Online Safety, in these lessons, and address any concerns promptly.

- The school provides opportunities within a range of curriculum areas and discrete Computing lessons to teach about Online Safety (in accordance with the Computing overview)
- Educating pupils to manage the risks when using technologies that maybe encountered outside school may also be done informally when opportunities arise.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them (this is age appropriate)
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities. (this is age appropriate)
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the

internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.
- Lessons are taught appropriately to each age range across the school ***(Please see Appendix A for more detailed information on learning objectives taught across the school)***

5. USE OF MOBILE PHONES AND SMART DEVICES BY PUPILS

Pupils are allowed to bring a mobile to school, *provided that they have signed permission in advance from their parent or carer and this has been agreed by a teacher or member of SLT.*

Permission may be granted in the event that pupils are:
-Travelling to school by themselves
-Young carers who need to be contactable

- All mobile phones/ smart watches must be handed to the class teacher to be placed in the teacher's cupboard. These should be on airplane mode or switched off.
- They can only disable airplane mode or switch them on once out of the school gates.
- No mobile phones/ smart watches should be on a pupil's person or belongings during the school day, unless permission has been granted in advance by a member of SLT for exceptional circumstances.
- Pupil mobile phones/ smart watches are not permitted on school trips or residentials.

6. PASSWORD SECURITY

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have access to this through Administrator Rights on the school network, as well as the SIMS registration system. The pupils from Year R upwards have class logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

7. DATA SECURITY

The accessing and appropriate use of school data is something that the school takes very seriously. Level of access is determined by the Headteacher and kept in line with GDPR regulations. The staff are aware of the importance of keeping the data private and that data should be kept in secure folders and files.

8. MANAGING THE INTERNET

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- In Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Staff will preview any recommended sites before use, including fully viewing the specific media content to be used (i.e. videos, audio etc.).
- Only school approved and child friendly sites are to be used when searching images. When searching for images on sites which are not as easily filtered (e.g. Google Images), staff must not perform the search in the view of pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- 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, including using the SWGFL filtering system to ensure effective and up-to-date filtering of inappropriate 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 LA 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.
- Staff must not discuss the school, parents, pupils or any aspects relating to the school when using online social media and are advised to wait until after an ex-pupil's 18th birthday before accepting any request on social media. Saint Patrick's School would advise staff not to accept any ex-pupil as a friend, on social media
- In general, the use of online chat for children will not be permitted other than as part of an online learning environment
- Social networking sites may be allowed for specific purposes, e.g. teaching Online Safety.
- Staff must be aware of the professional risks involved in using social networking and must take reasonable care to present themselves in a respectful and decent way, so as to maintain and uphold appropriate Personal and Professional Conduct (as outlined in the Teachers' Standards).
- The Headteacher will ensure that the Online Safety policy is implemented and compliance with the policy monitored.

9. INFRASTRUCTURE

- School internet access is controlled through the LA's web filtering service.
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the class teacher who must inform an Online Safety co-ordinator.
- It is the responsibility of the school, by delegation to the technical support; to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the School Business Manager.
- If there are any issues related to viruses or anti-virus software, the School Business Manager should be informed asap.

10. PERSONAL DEVICES (including mobiles, tablets, laptops , music players etc.)

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

- The school allows staff to bring in personal mobile phones and devices. However, these must be switched off and kept in a secure area during the school day.
- Staff are not permitted to take images, video or audio of a child using their own personal devices, but should instead use school devices.
- Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- Mobile phones of visitors and parents are not permitted to be used once in the school building, and posters are displayed as a reminder. Work experience students must leave their phones in the school office, where they will be safely stored.
- Pupils are not allowed to bring personal mobile devices/tablets/phones/games consoles/computers/etc. to school unless it is for educational purposes determined and consented to by the class teacher and Online Safety co-ordinator. In such cases, strict monitoring and controlled usage is essential. Year 6 can bring in a mobile phone if walking home unsupervised, but this must be handed to the class teacher at the start of the day and will be returned at the end of the school day.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

- Each class teacher is provided with a class iPad to be used a teaching tool. They may take the iPad out of school so as to utilise the apps and features. However, it must be used in an appropriate and safe way, as if it were a school computer or laptop.

11. MANAGING EMAIL

The use of email within most schools is an essential means of communication for both staff and pupils. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or internationally. We recognise that pupils need to understand how to style an email in relation to their age. In Key Stage 2 pupils will have experienced how to safely send and receive emails.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. This should be the account that is used for all school business.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arranging to meet anyone without specific permission.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
- Staff must inform the School Business Manager if they receive an offensive e-mail.

12. TAKING IMAGES AND FILM

Digital images are easy to capture, reproduce and publish and, therefore, easy to misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, this includes when on school trips. With the consent of the class teacher, pupils are permitted to take digital cameras and iPads from school to record images and can download these images on the school network.

13. PUBLISHING PUPILS' IMAGES AND WORK

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school website
- On the school Instagram Page
- On Google Classrooms / Tapestry Class page
- In the school advertising and other printed publications that the school may produce for promotional purposes
- Recorded/transmitted on a video or webcam
- In display material that may be used in the school's communal areas
- In display material that may be used in external areas, i.e. exhibition promoting the school
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

- Parents/carers may withdraw permission, in writing, at any time.
- E-mail and postal addresses of pupils will not be published.

14. STORAGE OF IMAGES

Images/ films of children are stored on the school's network.

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher.

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/Learning Platform

15. MISUSE AND INFRINGEMENTS

Complaints and Concerns

- Complaints relating to Online Safety should be made to the Headteacher (J. Courtney)
- All incidents will be logged and followed up.
- Complaints or concerns of a child protection nature must be dealt with in accordance with school Child Protection procedures and must be reported to the DSL or Deputy DSL.
- Pupils and parents will be informed of the complaints procedure.
- Parents and children and young people will need to work in partnership with practitioners to resolve issues should they arise.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the DSL (Jennie Courtney).

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Online Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher / Chair of Governors / LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct.

16. PUPILS WITH ADDITIONAL NEEDS

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.
Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people.

16. GENERATIVE ARTIFICIAL INTELLIGENCE

The school acknowledges the benefits of the use of AI in an educational context - including enhancing teaching and learning and outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.

- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Learners Safe
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will ensure that, within our education programmes, learners understand the ethics and use of AI and the potential benefits and risks of its use. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in acceptable use agreements, the school will use AI responsibly and with awareness of data sensitivity. Where used, staff should use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymized data to avoid the exposure of personally identifiable or sensitive information.
- Staff should always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.

- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognize and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.

POLICY REVIEW

The Governing Body will undertake an annual review of the school's Online Safety Policy as part of its review of Safeguarding Policies. The school will remedy any deficiencies or weaknesses found without delay.

Policy updated: October 2025
Date of next review: September 2026
Responsibility: Mrs Jennie Courtney (DSL)

APPENDIX A

E- safety Annual Programme

Term 1	Self-Image and Identity
Term 2	Online Bullying *As part of 'Anti-Bullying Week', Monday 10th-Friday 14th November
Term 3	Online Relationships *As part of 'Safer Internet Day'- Tuesday 10th February 2025
Term 4	Online Reputation
Term 5	Managing Online Information
Term 6	Privacy and Security Copyright and Ownership

Health, Well-being and Lifestyle