

St Joseph's Catholic Primary School



Our Mission Statement

We grow together in God's Love as we Pray, Learn and Play

"Dyn ni'n tyfu gyda'n gilydd mewn cariad Duw wrth i ni weddio, dysgu a chwarae"

INTERNET SECURITY AND ONLINE SAFETY POLICY

Article 32:

You have the right to be protected

Contents

1. Policy statement and ethos
2. Purpose and aims
3. Scope
4. Legal and policy framework
5. Understanding online safety risks
6. Development, monitoring and review
7. Roles and responsibilities
8. Online Safety Group
9. Acceptable use and expected conduct
10. Personal devices and mobile phones
11. Reporting and responding to incidents
12. Use of artificial intelligence
13. Online safety education
14. Staff and governor training
15. Working with parents, carers and the wider community
16. Filtering and monitoring
17. Technical security
18. Cyber security and incident response
19. Data protection and privacy
20. Device management and remote learning
21. Digital content, images, video and audio
22. Public online communications and social media
23. Outcomes and evaluation
24. Approval and review
 - Appendix 1: Online safety incident response
 - Appendix 2: Acceptable use summary
 - Appendix 3: Key contacts and roles
 - References and acknowledgements

Important: This policy should be read alongside the school's Safeguarding and Child Protection, Behaviour, Data Protection, Staff Code of Conduct, Social Media, Whistleblowing and Complaints policies.

1. Policy statement and ethos

St Joseph's R.C. Primary School recognises that digital technology, the internet and online services are essential to education, communication and participation in modern life. Used well, they enable creativity, collaboration, inclusion and access to learning. Used unsafely, they can expose children and adults to harm, abuse, exploitation, misinformation, discrimination, privacy breaches and cybercrime.

Our Catholic ethos requires every member of the community to uphold the dignity of the human person, act with truth, respect others and work for the common good. These principles apply equally online and offline. We aim to create a culture in which learners become ethical, informed citizens who use technology confidently, critically and responsibly.

Online safety is an integral part of safeguarding. It is not limited to computing lessons or technical controls. It is a whole-school responsibility reflected in leadership, curriculum design, staff conduct, family engagement, filtering and monitoring, cyber security, data protection and the way incidents are reported and managed.

2. Purpose and aims

The purpose of this policy is to establish a clear and proportionate framework for the safe, secure and responsible use of digital technology.

The school will:

- protect learners and adults from online harm while enabling positive and purposeful use of technology;
- set clear expectations for behaviour, professional conduct and acceptable use;
- provide a planned and progressive programme of online safety education through the Curriculum for Wales and the Digital Competence Framework;
- ensure concerns are reported, recorded, investigated and escalated promptly through safeguarding procedures;
- maintain appropriate filtering, monitoring, technical security, data protection and cyber security arrangements;
- support the safe and ethical use of artificial intelligence and emerging technologies;
- work in partnership with parents, carers, governors, the local authority, iTeach and relevant agencies;
- review practice regularly using evidence, learner voice, incident trends and the 360 safe Cymru self-review tool.

3. Scope

This policy applies to all members of the school community, including staff, learners, governors, volunteers, parents/carers, visitors, contractors and community users.

It covers:

- school-owned or school-managed devices, networks, accounts, systems and services;
- use of school systems on or off the school site, including home and remote learning;
- personal devices used on the school site or connected to school networks, where permitted;
- online behaviour outside school where it affects the safety, wellbeing, learning, reputation or orderly running of the school community;

- digital content, images, audio, video, messaging, social media, gaming, cloud services and artificial intelligence.

Where an online incident takes place outside school but has an impact on a learner or the school community, the school will respond in line with safeguarding, behaviour and anti-bullying procedures. Parents/carers will be involved where appropriate, and external agencies will be contacted when required.

4. Legal and policy framework

This policy is informed by relevant legislation and guidance applicable in Wales, including:

- Education Act 2002, including the duty on governing bodies and local authorities to safeguard and promote the welfare of children;
- Children Act 1989 and Children Act 2004;
- Social Services and Well-being (Wales) Act 2014 and the Wales Safeguarding Procedures;
- Welsh Government statutory guidance *Keeping learners safe*;
- Curriculum for Wales, including the mandatory cross-curricular skill of digital competence and the Digital Competence Framework;
- *Rights, Respect, Equality*: statutory anti-bullying guidance for governing bodies of maintained schools;
- Data Protection Act 2018 and UK General Data Protection Regulation;
- Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and relevant communications legislation;
- Equality Act 2010, Human Rights Act 1998 and Counter-Terrorism and Security Act 2015;
- Online Safety Act 2023, where relevant to the wider regulatory context for online services.

This policy should be read alongside the other school policies listed at the beginning of the document. Where different policies apply to the same incident, safeguarding and the immediate welfare of the child will take priority.

5. Understanding online safety risks

The school considers online risk through four connected areas. Risks may overlap and can affect children and adults in different ways.

Area	Examples
Content	Exposure to illegal, inappropriate or harmful material, including sexual content, violence, self-harm or suicide content, racism, misogyny, hate, extremist content, misinformation, disinformation and harmful AI-generated material.
Contact	Harmful interaction with other people, including bullying, coercion, grooming, exploitation, pressure from peers or adults, impersonation, unwanted contact and unsafe communication with strangers.
Conduct	Behaviour that causes or increases harm, including cyberbullying, oversharing, unsafe livestreaming, sharing nude or semi-nude images, harassment, abuse, copyright infringement, plagiarism, account misuse and bypassing security controls.
Commerce	Risks linked to gambling, in-app purchases, scams, phishing, fraud, misleading advertising, subscription traps, financial exploitation and the commercial collection or profiling of personal data.

The school also recognises risks created by rapid technological change, including deepfakes, synthetic media, AI companions, persuasive design, algorithmic bias, location tracking, smart devices and the misuse of publicly available images.

6. Development, monitoring and review

This policy is developed and reviewed through a whole-school approach involving senior leaders, the Designated Safeguarding Person, the Online Safety/Digital Competence Lead, iTeach as the school's IT provider, staff, governors and learner voice. Parents/carers may also be consulted where appropriate.

Monitoring the impact of the policy

The school will use the following evidence to evaluate effectiveness and identify improvement priorities:

- online safety, safeguarding, behaviour and bullying incident records;
- filtering and monitoring reports, alerts and requests for changes;
- network, account and cyber security information provided by iTeach;
- learner, staff and parent/carer surveys or discussions;
- curriculum mapping, learning evidence and learner outcomes;
- staff training records and confidence checks;
- 360 safe Cymru self-review evidence and action plans;
- lessons learned from incidents, audits, near misses and complaints.

The policy will be reviewed at least annually and sooner when there is a significant incident, a change in law or guidance, a major technology change, a new digital service, or evidence that current arrangements are not effective.

7. Roles and responsibilities

Online safety is a shared responsibility. Everyone is expected to model safe and respectful behaviour, protect information, follow agreed procedures and report concerns promptly.

7.1 Governing Body

The Governing Body will:

- approve this policy and provide strategic challenge and oversight;
- nominate a governor with responsibility for online safety or include the responsibility within the safeguarding governor's role;
- receive anonymised reports on incidents, education, filtering and monitoring, cyber security and policy implementation;
- seek assurance that filtering, monitoring, technical security and data protection arrangements are effective and reviewed;
- undertake appropriate safeguarding, online safety and basic cyber security training;
- ensure that sufficient resources, expertise and accountability are in place.

7.2 Headteacher and Senior Leadership Team

The Headteacher and Senior Leadership Team will:

- set a culture in which safeguarding and responsible technology use are prioritised;
- ensure this policy is implemented consistently and linked to relevant school policies;
- make sure the Designated Safeguarding Person, Online Safety Lead, staff and iTeach understand their responsibilities and receive appropriate training;
- receive regular reports, respond to emerging risks and ensure improvement actions are completed;
- oversee serious incidents and allegations involving staff, following local authority, safeguarding and human resources procedures;
- ensure new technologies and services are approved only after appropriate safeguarding, privacy, security and educational checks.

7.3 Designated Safeguarding Person

The Designated Safeguarding Person will:

- hold lead responsibility for safeguarding, including online safety;
- maintain current knowledge of online risks, harmful sexual behaviour, image-sharing, filtering and monitoring and relevant referral routes;
- coordinate the response to online safety concerns, record decisions and make safeguarding referrals where needed;
- liaise with the Headteacher, Online Safety Lead, iTeach, the local authority and external agencies;
- review incident patterns and monitoring information, ensuring support is appropriate for learners with additional learning needs;
- report key themes and actions to senior leaders and governors without identifying individuals unnecessarily.

7.4 Online Safety/Digital Competence Lead

The Online Safety/Digital Competence Lead will:

- support the Designated Safeguarding Person with day-to-day online safety practice while recognising that safeguarding accountability remains with the Designated Safeguarding Person;
- coordinate policy review, awareness activity and the 360 safe Cymru self-review process;
- map and evaluate online safety education across the curriculum;
- support staff confidence, learner voice, Digital Leaders and Safer Internet Day activities;
- maintain knowledge of risks across content, contact, conduct and commerce;
- liaise with curriculum leads, iTeach and pastoral staff.

7.5 iTeach – IT service provider and technical staff

iTeach will:

- maintain secure, managed infrastructure and role-appropriate user access;
- implement, maintain and test filtering, monitoring, malware protection, backups, updates and other security controls;
- provide timely reports, alerts and advice to the named school leads;

- support risk assessment and due diligence for new systems, services and devices;
- report misuse, weaknesses, suspected compromise or data incidents immediately;
- work within the school's policies and contractual data protection and security requirements.

The school remains accountable for online safety and data security when services are outsourced.

7.6 Teaching and support staff

Teaching and support staff will:

- follow this policy, the Staff Acceptable Use Agreement, safeguarding procedures and the Staff Code of Conduct;
- maintain professional boundaries in all online communication and use only approved accounts and services for school business;
- supervise learner use of technology, plan age-appropriate activities and respond calmly if unsuitable content is encountered;
- teach and model safe, respectful, critical and lawful use of digital technology;
- protect passwords, devices and personal data and report loss, compromise, phishing or accidental disclosure immediately;
- use only approved AI tools and check all AI-supported outputs for accuracy, bias, suitability and copyright;
- report any online safety or safeguarding concern without delay and preserve evidence only in accordance with advice.

7.7 Learners

Learners will:

- follow the age-appropriate Learner Acceptable Use Agreement and staff instructions;
- use school technology for learning and approved activities only;
- keep passwords private, respect the work and privacy of others and never attempt to bypass security controls;
- think carefully before creating, posting or sharing content and seek consent before recording others;
- tell a trusted adult if something online worries, upsets or frightens them, or if they see harmful or illegal content;
- use AI responsibly, acknowledge support where required and never use it to deceive, bully, impersonate or plagiarise;
- understand that online behaviour outside school may be addressed when it affects the school community.

7.8 Parents and carers

Parents and carers will be encouraged to:

- support the school's expectations for safe and responsible use;
- encourage age-appropriate use of devices, games, apps and services and discuss online experiences regularly;

- inform the school promptly about online incidents that may affect their child or the school community;
- respect school communication routes and avoid posting content that identifies or harms children, staff or families;
- support arrangements for learner mobile phones and personal devices;
- engage with guidance, workshops and acceptable use information provided by the school.

7.9 Visitors, volunteers, contractors and community users

Visitors, volunteers, contractors and community users must:

- follow staff instructions;
- use guest access only where authorised;
- protect confidential information;
- not photograph or record learners without permission;
- not communicate with learners through personal accounts;
- report any concern immediately to a member of staff or the Designated Safeguarding Person.

8. Online Safety Group

Online safety oversight may be carried out by a dedicated group or incorporated into the school safeguarding or digital strategy group.

Membership should normally include:

- the Designated Safeguarding Person;
- the Online Safety/Digital Competence Lead;
- a senior leader;
- the online safety governor;
- a representative from iTeach, where appropriate;
- teaching and support staff representatives;
- learner representatives.

Parent/carers representation may be included where appropriate.

The group will:

- review the policy, action plan and 360 safe Cymru evidence;
- consider anonymised incidents, trends, emerging risks and lessons learned;
- review filtering and monitoring arrangements and requests for changes;
- evaluate curriculum coverage, progression, inclusion and learner outcomes;
- promote learner voice, peer support and family engagement;
- report actions and impact to senior leaders and governors.

9. Acceptable use and expected conduct

School technology is provided to support education, safeguarding, communication and administration. Access is a privilege and must be used lawfully, safely, respectfully and in accordance with school instructions.

Acceptable Use Agreements provide age-appropriate and role-appropriate detail and are reinforced through induction, teaching, posters, reminders and staff supervision.

9.1 Core expectations

All users must:

- use only the account allocated to them and keep passwords and authentication codes secure;
- use school systems and internet access for approved educational or professional purposes;
- communicate respectfully and not bully, harass, threaten, discriminate against, impersonate or deliberately embarrass others;
- not create, access, store, request, upload or share illegal, sexual, violent, hateful, extremist or otherwise harmful material;
- not attempt to bypass filtering, monitoring, device management or network security using VPNs, proxies, alternative DNS, unauthorised extensions or other methods;
- not install software, connect devices, alter settings, run scripts or use removable media without permission;
- respect copyright, licensing and intellectual property;
- cite sources and acknowledge AI support where required;
- not reveal confidential information or enter personal data into unapproved websites, applications or AI services;
- report accidental access to unsuitable content, suspicious messages, lost devices, compromised accounts or security weaknesses immediately;
- not use school systems for private business, gambling, financial gain, unauthorised fundraising or unlawful activity.

9.2 Illegal or serious activity

The following will be treated as safeguarding and/or criminal concerns and escalated immediately:

- child sexual abuse material, grooming, exploitation or sexual coercion;
- non-consensual intimate images, including the creation or distribution of sexualised deepfakes;
- terrorism-related material, serious threats, incitement to violence or hate crime;
- content encouraging or assisting suicide or serious self-harm;
- fraud, extortion, phishing, credential theft or unauthorised access;
- creating or spreading malware, ransomware or harmful scripts;
- deliberately disrupting networks, services or devices;
- sale or promotion of illegal substances, weapons or other unlawful goods.

Evidence and illegal imagery: Staff must not copy, print, forward, download, save, screenshot or unnecessarily view suspected illegal or intimate imagery. The device should be secured and the

Designated Safeguarding Person informed immediately. The school will follow safeguarding and police advice and will not conduct its own criminal investigation.

9.3 School-specific acceptable use

Activity	Staff and other adults	Learners
Online gaming and in-game communication	Only for an approved educational purpose or authorised staff wellbeing activity. No personal gaming on school systems during working time.	Only when teacher-directed, age-appropriate and supervised. Public chat and voice functions must be disabled where possible.
Online shopping and commerce	Only nominated staff may make authorised purchases for school business. Personal shopping must not use school accounts or payment details.	Not permitted.
Cloud storage and file sharing	School-approved services and school accounts only. Sensitive information must be shared using approved secure methods.	School-approved services only, under staff direction. Peer-to-peer and torrent services are not permitted.
Social media and user-generated platforms	Only authorised staff may manage official accounts. Personal accounts must not be used to contact learners or conduct school business.	Not permitted on school systems unless an age-appropriate platform is specifically approved and teacher-directed.
Messaging, chat and voice	School-approved platforms and accounts only for professional communication. No personal messaging with learners.	Approved learning platforms only, with staff oversight and appropriate settings.
Streaming, video platforms and livestreaming	Permitted for a legitimate professional or curriculum purpose after suitability checks. Personal entertainment use is not permitted during directed time.	Teacher-selected, age-appropriate content only. Learners must not livestream from school.
Personal phones, smartwatches and earbuds	Restricted to designated times and areas and must not interfere with duties. They must not be used to photograph or record learners.	May be brought only where agreed for safety or travel. Devices must be switched off and handed to staff or the office for secure storage. No use during the school day.
Photographs, video and audio	School devices and approved storage must be used. Consent, safeguarding and data protection requirements must be followed.	Only as part of a teacher-directed activity using an approved device. Consent and respectful use are required.
Personal email	Must not be used for school business. Limited personal access should be on a personal device during breaks and must not compromise security or duties.	Not permitted on school systems.
School email	For professional purposes. Incidental use must be reasonable, lawful and not commercial.	For learning and school communication only, where accounts are provided.

Artificial intelligence	Only approved tools and accounts may be used. Personal, confidential or sensitive data must not be entered. Human checking and professional accountability are required.	Only approved tools may be used, when age requirements are met and under staff direction. Deception, harmful content and plagiarism are not permitted.
USB drives and removable media	Only approved, scanned and, where required, encrypted media may be used.	Only with staff permission.

10. Personal devices and mobile phones

The school operates a pupil device-free approach during the school day. This includes mobile phones, smartwatches, earbuds and other connected personal devices.

Learners

- A learner may bring a phone only when it is necessary for safe independent travel and the school has received parental permission.
- The device must be switched off before entering the school and handed to the class teacher or school office for secure storage.
- The device is collected at the end of the school day and must not be used on site unless a senior member of staff authorises emergency use.
- Smartwatches and connected wearables follow the same rule.
- Where a device cannot be switched off or prevents safe supervision, it must remain at home.
- The school is not responsible for loss or damage to unauthorised personal devices.
- Misuse may result in confiscation in line with school policy, parental contact, withdrawal of permission and further safeguarding or behaviour action.

Staff, visitors and volunteers

- Personal devices must be on silent and kept away while supervising or teaching unless required for an authorised purpose.
- Personal devices must not be used to photograph, film or record learners, school records or confidential information.
- Staff must use school-approved communication systems rather than personal telephone numbers, social media or messaging accounts.
- Visitors and volunteers must follow staff instructions and keep devices away unless authorised.

11. Reporting and responding to incidents

The school is committed to a reporting culture in which concerns are taken seriously and no one is discouraged from speaking.

Learners will be reminded that they can tell any trusted adult and will not be blamed for reporting something that has happened to them.

11.1 Reporting routes

- **Learners:** Tell a trusted adult, class teacher, teaching assistant, Designated Safeguarding Person, Headteacher or another member of staff.
- **Staff and volunteers:** Report immediately to the Designated Safeguarding Person. Concerns about a member of staff must be reported to the Headteacher. Concerns about the Headteacher must be reported to the Chair of Governors in line with the safeguarding policy.
- **Parents/carers:** Contact the school office, class teacher, Designated Safeguarding Person or Headteacher using the school's official communication routes.
- **Technical concerns:** Report to the designated school lead and iTeach without delaying a safeguarding report.

11.2 Immediate response

1. Take any immediate action needed to protect a child or adult from harm.
2. Listen calmly, reassure the person reporting and avoid asking leading or investigative questions.
3. Do not promise confidentiality. Explain that information will be shared only with people who need to help.
4. Inform the Designated Safeguarding Person without delay and record the concern accurately using the school safeguarding system.
5. Preserve potential evidence without forwarding, copying or repeatedly viewing it. Secure the device if advised.
6. Do not contact an alleged offender or carry out a criminal investigation unless directed by the Designated Safeguarding Person and relevant agencies.
7. Consider the wellbeing and support needs of all children involved, including the person harmed, the person alleged to have caused harm and any witnesses.

11.3 Assessment, escalation and external support

The Designated Safeguarding Person and Headteacher will assess the concern using safeguarding procedures.

Suspected illegal content, serious harm or immediate danger will be escalated to the police, social services, the local authority safeguarding team or another appropriate agency.

Advice may also be sought from:

- CEOP;
- the UK Safer Internet Centre Professionals Online Safety Helpline;
- Report Harmful Content;
- the local authority;
- the police;
- social services.

Where an incident involves a member of staff, volunteer or other adult, the school will follow the managing allegations and safeguarding procedures and seek local authority designated officer and human resources advice.

Any suspension or restriction will be a neutral safeguarding measure and not a presumption of guilt.

11.4 Recording and monitoring

- All concerns, decisions, actions, referrals and follow-up will be recorded securely and confidentially.
- Online safety incidents will be reviewed for patterns, repeated behaviours, vulnerable groups and curriculum or technical lessons.
- Anonymised themes will be reported to senior leaders, governors and the Online Safety Group.
- Parents/carers will be informed when appropriate, unless doing so could place a child at greater risk or prejudice an investigation.
- Incidents will be managed proportionately through safeguarding, behaviour, anti-bullying, disciplinary or complaints procedures, as applicable.

11.5 Responding to learner actions

Incident or behaviour	Typical school response
Accidental access to unsuitable content	Reassure the learner, close or minimise the content, report it to staff, record it if necessary, review filtering arrangements and provide further education.
Online bullying, harassment or discrimination	Complete a safeguarding assessment, support those affected, preserve evidence, contact parents/carers, apply an appropriate restorative or behaviour response and make an external referral if serious.
Sharing personal information or unsafe contact	Protect accounts, block or report the contact, support the learner, inform parents/carers where safe, review privacy arrangements and consider a safeguarding referral.
Sharing nude or semi-nude images	Follow safeguarding and UKCIS guidance. Do not view or copy images. Secure devices, support children, assess coercion or exploitation and involve the police or social services when required.
Bypassing filters, account misuse or cybercrime	Secure systems, preserve logs, restrict access if necessary, notify iTeach and parents/carers, provide education and consider police or National Crime Agency referral for serious or repeated conduct.
Repeated or serious misuse	Complete an individual risk assessment, introduce a safeguarding and behaviour plan, proportionately restrict access, hold a parental meeting and seek specialist support or referral.

11.6 Responding to staff actions

Incident or behaviour	Typical school response
Accidental error or minor breach	Report immediately, secure the information, assess the risk, record the incident, correct the issue and provide advice or training.
Professional boundary concern	Report to the Headteacher or Designated Safeguarding Person, safeguard learners, preserve evidence and follow managing allegations or disciplinary procedures.

Data protection or security breach	Contain the breach, inform the Data Protection Officer and iTeach, assess notification requirements, document decisions and implement remedial action.
Access to illegal or harmful material	Secure the system or device, do not investigate, notify the Headteacher and Designated Safeguarding Person and seek police or local authority advice. Disciplinary procedures may apply.
Failure to report or repeated breach	Formal management action or disciplinary procedures may be used, depending on seriousness, intent, impact and previous guidance.

12. Use of artificial intelligence

Artificial intelligence, including generative AI, may support learning, teaching and administration when it is used safely, ethically and purposefully.

It must not replace:

- professional judgement;
- relationships between staff and learners;
- safeguarding decisions;
- the teacher's responsibility for the quality and accuracy of work.

12.1 Approval and risk assessment

- Only school-approved AI services, accounts and features may be used for school purposes.
- Before a new AI tool is introduced, the school will consider its educational value, age restrictions, safeguarding, privacy, security, accessibility, bias, copyright, data location, retention and whether a Data Protection Impact Assessment is required.
- The Data Protection Officer and iTeach will be consulted where the proposed use may involve personal data, special-category data, automated decision-making or integration with school systems.
- The school will maintain a register of approved AI tools and their agreed purposes.

12.2 Safe staff use

- Staff must not enter names, images, identifiable pupil work, safeguarding information, assessment data, health information, contact details, confidential documents or other personal or sensitive data into public or unapproved AI tools.
- AI outputs must be checked for accuracy, bias, harmful content, age suitability, copyright and alignment with the Curriculum for Wales and the school's Catholic ethos.
- Staff remain accountable for any AI-supported resource, communication, plan, assessment or decision.
- AI must not make the sole decision in safeguarding, admissions, behaviour, staffing, assessment, additional learning needs or any matter with a significant effect on an individual.
- Where AI has materially shaped a published document or learner task, staff should be transparent where appropriate.
- Staff must not use AI to impersonate a person, fabricate evidence, create misleading images, audio or video, or generate content that could cause harm or bring the school into disrepute.

12.3 Learner use

- Learners may use AI only when a teacher has approved the tool, task and level of support and when the service's age requirements are met.
- Learners will be taught that AI can produce inaccurate, biased or fabricated information and that important information must be verified using reliable sources.
- Learners must not enter personal information about themselves or others, upload identifiable images or share confidential school information.
- AI use must be acknowledged when required.
- Submitting AI-generated work as entirely one's own is plagiarism and will be addressed as a learning and behaviour matter.
- Creating sexualised, violent, discriminatory or humiliating AI content, including deepfakes or impersonation, is prohibited and may be treated as a safeguarding or criminal matter.

12.4 Assessment and feedback

AI may assist staff to:

- identify patterns;
- draft questions;
- adapt resources;
- suggest feedback.

Teachers must always make the final professional judgement.

Learner work, reports and assessment information must not be uploaded to an AI service unless the use has been approved and data protection requirements have been met.

13. Online safety education

The school will provide a planned, progressive, inclusive and regularly reviewed programme of online safety education.

It will be embedded across the Curriculum for Wales, particularly through:

- the Digital Competence Framework;
- Health and Well-being;
- Relationships and Sexuality Education;
- Science and Technology;
- Humanities;
- Languages, Literacy and Communication;
- assemblies;
- pastoral provision.

Learning will be age-appropriate, revisited regularly and adapted for learners with additional learning needs. It will develop knowledge, skills, critical thinking and confidence to seek help.

Core curriculum content

Online safety education will include:

- privacy, personal data, passwords, authentication, digital footprints and online reputation;
- respectful communication, consent, healthy relationships, cyberbullying, harassment and bystander action;
- grooming, exploitation, coercion, unsafe contact and how to block, report and seek help;
- reliable information, misinformation, disinformation, scams, persuasive design and checking sources;
- age restrictions, gaming, livestreaming, gambling-like features, in-app purchases and commercial risks;
- copyright, intellectual property, plagiarism and ethical use of AI;
- self-generated intimate images, image-based abuse and the risks of deepfakes, taught sensitively and in line with safeguarding guidance;
- cyber security, phishing, malware, account security and the Computer Misuse Act;
- wellbeing, screen use, sleep, body image, harmful content and strategies for managing online pressure;
- clear reporting routes and trusted sources of help.

Teachers will guide learners to suitable resources and supervise open searching.

If unsuitable content is encountered, learners will be supported to stop, close or minimise it and report it immediately.

Legitimate requests to adjust filtering for curriculum use must be authorised, time-limited and auditable.

Learner voice

The school will use:

- learner feedback;
- the School Senedd;
- Digital Leaders;
- surveys;
- class discussions.

This information will help the school understand current experiences, identify emerging issues and improve education and reporting routes.

Learners may help to create campaigns, assemblies and family guidance, but they will not be asked to manage safeguarding incidents.

14. Staff and governor training

Staff and volunteers

- Online safety will be included in safeguarding induction before staff or volunteers have unsupervised access to learners or school systems.
- All staff will receive regular safeguarding and online safety updates, normally at least annually, with additional briefings when risks or systems change.

- Training will include reporting routes, professional boundaries, filtering and monitoring, data protection, phishing and cyber security, mobile devices, images, remote learning and approved AI use.
- The Designated Safeguarding Person and Online Safety Lead will maintain enhanced knowledge through appropriate local authority, Hwb, SWGfL, UK Safer Internet Centre or other recognised training.
- Training needs will be reviewed using incident evidence, audits, staff feedback and changes in technology.

Governors

- Governors will receive safeguarding and online safety awareness appropriate to their strategic role.
- The nominated governor will receive enhanced understanding of filtering and monitoring, cyber security and how to challenge and support leaders.
- Governors will receive regular anonymised updates on implementation, risks and impact.

15. Working with parents, carers and the wider community

Parents and carers are essential partners in helping children build safe and balanced online habits.

The school will communicate in a supportive and non-judgemental way and recognise that technology and family circumstances vary.

The school will:

- publish this policy and make acceptable use expectations clear;
- share timely guidance through the website, ClassDojo or other approved communication channels, newsletters, meetings and campaigns;
- provide information about reporting, parental controls, privacy, games and apps, scams, social media, AI and emerging risks;
- offer workshops, drop-in sessions or signposting to trusted resources where possible;
- seek permissions for digital services and images where required and explain how data will be used;
- promote Safer Internet Day and other relevant awareness activities;
- work with local schools, the local authority, police, health professionals, faith and community partners where this strengthens support.

The school will not expect parents/carers to investigate incidents themselves or circulate harmful content.

Parents/carers should preserve the device or message where safe, avoid forwarding material and contact the school or police as appropriate.

16. Filtering and monitoring

Filtering and monitoring are safeguarding measures that reduce risk but do not replace education, supervision, reporting or professional judgement.

Arrangements will be proportionate to:

- the age and needs of learners;
- the school's systems;

- the activities taking place.

The school will ensure that:

- illegal and known harmful content is blocked and age-appropriate and role-appropriate access is provided;
- web filtering includes appropriate protection for images and video as well as text-based content;
- monitoring supports timely identification of safeguarding and security concerns and is subject to human review;
- school-owned or managed devices are filtered and monitored on site and, where technically feasible, when used off site;
- staff and learners understand that activity on school systems may be logged and reviewed for safeguarding, security and compliance;
- the Designated Safeguarding Person, senior leaders, governors and iTeach have clear responsibilities for oversight;
- effectiveness is reviewed at least annually and after significant incidents, system changes or evidence of gaps;
- requests to unblock content are recorded, risk-assessed, approved by an authorised person and reviewed;
- monitoring information is accessed only by authorised people and handled confidentially.

Over-blocking will be addressed so that legitimate learning is not unnecessarily restricted.

No filtering or monitoring system is completely effective. Users must report unsuitable content or gaps immediately.

17. Technical security

The school and iTeach will maintain secure, reliable and well-managed infrastructure. Controls will be proportionate to risk and reviewed regularly.

The following arrangements will apply:

- Each user will have a unique account with role-based permissions and least-privilege access.
- Strong passwords and multi-factor authentication will be used where available and appropriate, especially for staff, administrators and remote access.
- Default accounts and passwords will be changed or disabled.
- Access will be removed promptly when a person leaves or changes role.
- Devices, servers, networks, operating systems, browsers and applications will be securely configured, patched and supported.
- Anti-malware, endpoint protection, firewall and device-management controls will be maintained.
- Administrator rights will be restricted to authorised users.
- Technical actions will be logged where possible.
- Remote access will be approved, secured and used only through authorised services.

- Backups of critical data and systems will be protected, tested and capable of restoration.
- Security weaknesses, lost devices, suspected compromise and unusual system behaviour must be reported immediately.
- Procurement and contracts will include appropriate security, privacy, support, data-return and deletion requirements.

18. Cyber security and incident response

Cyber security is a leadership and governance responsibility because incidents can disrupt learning, compromise safeguarding information and expose personal data.

The school will work to prevent, detect, respond to and recover from cyber threats.

Prevention and preparedness

The school will:

- maintain an up-to-date record of critical systems, suppliers, accounts and key contacts;
- train staff to recognise phishing, suspicious attachments, fraudulent payment requests, impersonation and social engineering;
- protect email and important accounts using multi-factor authentication and secure recovery methods where available;
- maintain segregated or otherwise ransomware-resistant backups and test restoration regularly;
- include cyber incidents in the school risk register, business continuity plan and emergency contact arrangements;
- review supplier assurance and clarify responsibilities for incident support, notification and recovery.

If a cyber incident is suspected

1. **Stop and report:** Users should stop the activity and contact the named school lead and iTeach immediately.
2. **Contain:** Authorised staff may isolate a device or account but should not delete evidence or attempt unsupported technical fixes.
3. **Protect people and data:** The Designated Safeguarding Person and Data Protection Officer will be involved where safeguarding or personal data may be affected.
4. **Escalate:** The school will contact the local authority, service providers, police, Action Fraud or other agencies as appropriate.
5. **Communicate:** The school will provide accurate, proportionate information to staff, families and governors without compromising an investigation.
6. **Recover and learn:** The school will restore systems from trusted backups, reset credentials, document decisions and update controls, training and continuity plans.

Ransomware: The school will not make or authorise a ransom payment without following local authority, police, insurer and legal advice. Priority will be given to safeguarding, containment, lawful reporting and recovery from trusted backups.

19. Data protection and privacy

Personal data will be processed lawfully, fairly, transparently and securely in accordance with UK GDPR, the Data Protection Act 2018 and the school's Data Protection Policy.

Children require particular protection because they may be less aware of risks and consequences.

The school will ensure that:

- a Data Protection Officer is appointed and provides advice and independent oversight;
- only the minimum personal data necessary for a clear purpose is collected, used, shared and retained;
- privacy notices explain how information is used and how rights can be exercised;
- data is stored and transferred using approved secure systems;
- access is limited to those who need it;
- personal data is not stored on unapproved personal devices, personal cloud accounts, removable media or consumer messaging services;
- new technology, applications, cloud services, AI tools and high-risk processing are subject to due diligence and a Data Protection Impact Assessment where required;
- images and videos are managed in accordance with privacy information, lawful basis, consent where appropriate and safeguarding considerations;
- data breaches are contained, recorded and reported promptly to the Data Protection Officer;
- the school assesses whether the Information Commissioner's Office and affected individuals must be notified;
- records are retained and securely deleted in accordance with the school retention schedule;
- staff receive regular data protection training and understand how to handle subject access requests, information requests and accidental disclosure.

20. Device management and remote learning

School-managed devices

- Devices will be inventoried, configured, updated and managed by authorised staff or iTeach.
- Learners will use devices under staff direction and must not remove profiles, install software, change security settings or share devices or accounts inappropriately.
- Devices taken home remain subject to this policy, acceptable use requirements, filtering and monitoring and return arrangements.
- Loss, theft, damage or suspected compromise must be reported immediately.
- Remote lock or wipe may be used where available.
- Shared devices will be signed out where appropriate and checked before reissue.

Remote and online learning

- Only school-approved platforms and school accounts will be used.
- Staff will maintain professional boundaries, use suitable locations and backgrounds and avoid sharing personal contact details.
- Learners and families will receive clear expectations about attendance, communication, camera and microphone use, recording, appropriate dress and behaviour.

- Live sessions will be planned so that another adult is aware of the session.
- One-to-one contact will take place only where necessary and in accordance with safeguarding arrangements.
- Sessions must not be recorded, photographed or shared unless the school has authorised this for a clear purpose and privacy requirements have been met.
- Concerns arising during online learning will be reported and managed through normal safeguarding procedures.

21. Digital content, images, video and audio

Digital content can enrich learning and celebrate achievement, but public sharing can create lasting safeguarding, privacy and reputational risks.

The school will apply a cautious, child-centred approach.

- Staff will use school devices and approved storage to create and manage learner images, video and audio.
- The purpose, lawful basis and audience will be considered before content is captured or published.
- Consent will be sought where required and preferences will be respected.
- Content will avoid unnecessary personal information, precise location data, sensitive context or combinations that make a child easier to identify or target.
- Public images will be selected and presented carefully.
- The school may reduce image resolution, limit close-up individual images, avoid full names and use group or activity-focused images where appropriate.
- Learners will be taught to seek consent, respect refusal and avoid humiliating, sexualised, coercive or unsafe recording and sharing.
- Images or recordings must not be copied to personal accounts, personal devices or unapproved services.
- Where misuse, manipulation or a deepfake is identified, the school will preserve appropriate evidence, support the person affected, request removal or report the content and consider a safeguarding or police referral.
- Copyright, licensing, accessibility and attribution requirements apply to all digital content.

22. Public online communications and social media

The school uses approved online channels to inform families, celebrate learning and engage with the community.

Official accounts are school assets and will be managed carefully.

- Only authorised staff may create, access or publish through official school accounts.
- Account ownership, administrator access, passwords, multi-factor authentication and recovery details will be recorded securely.
- Published content must be accurate, respectful, accessible and consistent with safeguarding, data protection, copyright and the school's Catholic ethos.
- Staff must not communicate with current learners through personal social media, personal messaging or personal email accounts.

- Staff should maintain professional judgement on personal accounts, use privacy settings and avoid content or discussion that could compromise professional standing, confidentiality or trust.
- School communication with parents/carers will use approved systems such as official email, telephone, ClassDojo or other authorised platforms.
- Comments, direct messages and public responses will be monitored proportionately.
- Abuse, threats, safeguarding concerns and misinformation will be recorded and escalated where necessary.
- The school may request removal of content that unlawfully identifies, harasses or endangers a learner or staff member and may involve platform reporting routes or external agencies.

23. Outcomes and evaluation

The school will evaluate whether this policy is improving safety, confidence and responsible participation rather than relying only on the number of reported incidents.

An increase in appropriate reporting may reflect greater trust and awareness.

Expected outcomes include:

- learners can recognise common online risks, make safer choices and know how to seek help;
- staff understand their responsibilities and respond consistently and promptly;
- parents/carers understand expectations and know where to obtain support;
- filtering, monitoring and technical controls are effective without unnecessarily restricting learning;
- personal data and school systems are protected and recoverable;
- AI and emerging technologies are introduced through proportionate risk assessment and human oversight;
- learning from incidents leads to changes in education, systems, policies or support;
- governors receive sufficient evidence to challenge, support and assure the school's approach.

Findings will inform:

- the school improvement plan;
- safeguarding priorities;
- curriculum planning;
- staff development;
- future policy reviews.

Appendix 1: Online safety incident response

1. Protect

Take immediate action to keep children and adults safe. Call the emergency services if there is immediate danger.

2. Report

Inform the Designated Safeguarding Person immediately. Concerns about staff must follow the managing allegations route.

3. Preserve

Secure devices or accounts only as advised. Do not forward, copy, print, download, screenshot or unnecessarily view harmful or illegal material.

4. Assess and escalate

The Designated Safeguarding Person or Headteacher will assess safeguarding risk and contact social services, the police, local authority, Data Protection Officer, iTeach or other agencies as required.

Staff must not conduct a criminal investigation.

5. Support

Provide appropriate support to:

- the person reporting;
- the person harmed;
- witnesses;
- any child alleged to have caused harm.

6. Record and inform

Record facts, decisions, actions and advice. Inform parents/carers where appropriate and safe.

7. Review and learn

Review filtering, supervision, curriculum, training, systems and policy. Monitor the situation and report anonymised themes to leaders and governors.

Appendix 2: Acceptable use summary

We will	We will not
Use school technology for learning and approved work.	Use school technology for illegal, harmful, sexual, hateful, commercial or unauthorised activity.
Use only our own accounts and keep passwords private.	Share accounts, guess passwords or access another person's files.
Be kind, respectful and truthful online.	Bully, threaten, discriminate against, impersonate or deliberately embarrass others.
Protect personal information and ask before recording or sharing.	Post names, images, locations or private information without permission.

Use approved websites, applications, storage and AI tools.	Install software, use VPNs or proxies or bypass filtering and monitoring.
Check information and AI outputs carefully.	Copy work, present AI output as our own or share misinformation.
Tell a trusted adult if something worries us or goes wrong.	Hide incidents, delete evidence or forward harmful content.
Look after devices and report loss or damage.	Alter settings, damage equipment or connect unauthorised devices.

References and acknowledgements

This policy has been adapted for a maintained primary school in Wales from the SWGfL/360 safe School Online Safety Policy Template supplied by the user and aligned with guidance and resources from:

- Welsh Government – *Keeping learners safe*;
- Hwb – online safety policies and procedures;
- Hwb – Digital Competence Framework;
- Hwb – web filtering and online safeguarding;
- Hwb – generative artificial intelligence in education;
- Hwb – keeping learners safe when using generative AI;
- Hwb – safeguarding principles and practice for online learning;
- Information Commissioner’s Office – children’s information and UK GDPR guidance;
- National Cyber Security Centre – cyber security guidance for schools and small organisations;
- UK Safer Internet Centre – professional support and reporting resources.

Copyright acknowledgement: SWGfL permits schools and educational institutions to use its policy templates for policy review and development.

This adapted policy should be reviewed against the school’s current systems, staffing, local authority arrangements and related policies before approval.

ALN

St Joseph's RC Primary School is committed to providing an inclusive learning environment in line with the Additional Learning Needs and Education Tribunal (Wales) Act 2018 and the ALN Code for Wales 2021. We are dedicated to identifying, assessing, and making provision for Additional Learning Needs at the earliest opportunity, working in collaboration with pupils, parents, and relevant professionals. Our approach is based on promoting equity, respecting diversity, and ensuring that all pupils are provided with opportunities to meet success.