Federation of St Charles and St Mary's Catholic Primary Schools

Computing and Online Safety Policy (2026)

Date policy adopted: October 2026

Review date: October 2027

The School Governors Federation Ethos Statement

As Governors we acknowledge our responsibilities as strategic leaders to ensure every child, in St Charles' and St Mary's Schools, are given the best possible opportunities to reach their full potential, spiritually and academically. We do this by promoting high standards of educational achievement, pastoral care and by modelling of the values proclaimed in the Gospel in both communities.

We are strongly committed to building and strengthening the shared Catholic ethos of both schools whilst maintaining their individual identities.

We strive to build on the values started at home and seek to provide an environment where beliefs and the ethos of the Catholic faith are taught, explored, developed and nurtured. We aim for all our children to believe in their own potential, in an environment where they can flourish, succeed and achieve.

As a governing body we have a strong focus on three core strategic functions:

- Ensuring clarity of vision, ethos and strategic direction which aim to deliver high expectations and to improve the lives and outcomes of all students.
- Holding the Executive Head Teacher and both Heads of School, to account for the educational performance of the school and its pupils, and for ensuring excellent quality of teaching.
- Overseeing the financial performance of the school and making sure its money is well spent.

As governors, we bring a wide variety of experience and expertise to the schools, and this ensures that both schools move forward and standards are constantly raised in a way that is in line with the overarching ethos and vision of the schools, along with the statutory directives from the Department for Education and The Archdiocese of Westminster.

Federation Motto: Together in faith, we love and learn

2. Aims and Objectives

The aim of this policy is to ensure that Computing and online learning at St Charles and St Mary's are taught in a way that develops curiosity, creativity and responsibility.

Our objectives are to:

- Deliver a broad, balanced and progressive Computing curriculum that meets the requirements of the National Curriculum and reflects each school's Catholic ethos.
- Equip pupils with the skills and confidence to use technology purposefully, creatively and safely.
- Encourage pupils to explore technology as independent thinkers and problem-solvers.
- Ensure that online behaviour reflects respect, compassion and responsibility, mirroring Gospel values.
- Enable pupils to understand and apply the key principles of computer science, information technology and digital literacy.
- Teach pupils how to keep themselves and others safe online through age-appropriate curriculum content and digital literacy initiatives, in line with Keeping Children Safe in Education (KCSIE) and the Department for Education's current Filtering and Monitoring Standards.
- Provide all staff with the guidance, resources and training required to teach Computing effectively and confidently and to recognise, respond to and report online-safety concerns.
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, governors and visitors.
- Identify and support groups of pupils who may be at greater risk of harm online, including pupils with SEND and other pupils who may require additional or personalised support.
- Deliver an effective approach to online safety which empowers the whole school community to use technology safely, responsibly and positively, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene in and escalate online-safety concerns and incidents, including concerns identified through filtering and monitoring systems.

3. Legislation and Guidance

This policy is based on the statutory safeguarding guidance, Keeping Children Safe in Education (KCSIE), from the Department for Education (DfE), and its advice for schools on:

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation
- Mobile phones in schools
- Filtering and monitoring

It also takes account of DfE guidance relating to protecting children from radicalisation and the safe and responsible use of artificial intelligence in education.

The policy reflects relevant legislation, including the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Education Act 2011, the Equality Act 2010, the Children's Wellbeing and Schools Act 2026, the UK General Data Protection Regulation, the Data Protection Act 2018 and the Data (Use and Access) Act 2025.

The policy also takes into account the National Curriculum programmes of study for Computing and the Department for Education's current Filtering and Monitoring Standards.

4. The 4 Key Categories of Online Risk

Our approach to online safety is based on addressing the following categories of risk. While some of these risks are more relevant to older children and teenagers, we teach age-appropriate awareness from the earliest years:

- Content – being exposed to inappropriate or harmful material online, such as violent images, content promoting discrimination or hatred, material encouraging self-harm, age-inappropriate content, and misleading or false information
- Contact – being subjected to harmful online interaction with others,

such as pressure from peers, contact from adults who may wish to harm or exploit children, or inappropriate commercial advertising
- Conduct – online behaviour that could cause harm to the child or others, such as sharing personal information, unkind messages or images, or being pressured to share images they're uncomfortable with
- Commerce – risks such as inappropriate advertising, being persuaded to spend money online, or being tricked into sharing personal or financial information

Our approach in primary school: We teach children age-appropriate awareness of these risks through our Computing and PSHE curriculum. For our youngest children, this means understanding how to be kind online, keeping personal information private, and knowing who to talk to if something worries them. As children progress through the school, we build their understanding of online risks in a developmentally appropriate way, always ensuring they feel empowered rather than frightened.

5. Curriculum Overview

At St Charles and St Mary's, Computing prepares pupils for a rapidly changing digital world. Our approach develops computational thinking, creativity, and safe, responsible use of technology, grounded in Catholic values.

The schools follow the Kapow Primary Computing Scheme across Key Stage 1 and Key Stage 2

This provides a clear progression of knowledge and skills through three strands:

- Computer Science – programming, algorithms, systems and networks.
- Information Technology – creating, storing and presenting digital content.
- Digital Literacy – responsible, respectful and confident use of technology.

The Kapow scheme also embeds online-safety objectives mapped to *Education for a Connected World (UKCIS 2023)* and ensures that all statutory elements of the National Curriculum are fully met.

Computing in the Early Years

In the Early Years Foundation Stage, children explore technology through play and guided experiences. They use programmable toys, simple apps and interactive media to develop logical thinking, communication and creativity.
These early experiences build curiosity and confidence that support later learning in Computing.

Cross-Curricular Integration

Computing at St Charles and St Mary's is not only taught in isolation.

Digital skills are woven through other subjects — for example, data handling in science, digital art and music, publishing work in English, and research in History and Geography.

This strengthens understanding and supports communication and collaboration across the curriculum.

Cultural Capital and Faith Context

Our Computing curriculum enhances pupils' cultural capital by exposing them to a wide range of technologies, problem-solving opportunities and creative media. Pupils learn how technology influences society and how to use it ethically to serve others, protect creation and promote justice, in keeping with Catholic social teaching.

6. Teaching, Learning and Assessment

Teaching and Learning

Computing at St Charles and St Mary's is taught using a practical, creative and inclusive approach. The Kapow Primary Computing Scheme provides carefully sequenced units which ensure full National Curriculum coverage and clear progression in skills, knowledge and understanding.

- Computing units are delivered over the course of a half term, following the curriculum map, with additional opportunities for pupils to use technology across the wider curriculum.
- Teachers adapt Kapow units to meet pupils' needs
- Activities are designed to be engaging and challenging, encouraging pupils to work independently and in teams.
- Pupils' work is recorded in Computing books or saved digitally as appropriate, providing evidence of learning and progress.
- Adaptation ensures that all pupils, including those with SEND, can access the curriculum successfully.
- Online safety is explicitly taught within Kapow units and revisited through PSHE, RSE and assemblies.

Assessment

Assessment in Computing is continuous and formative.

Teachers use Kapow's progression statements to monitor pupils' attainment and identify next steps.

Evidence includes:

- Annotated work in Computing books;
- Observations and discussion;
- Digital artefacts such as presentations, animations and code;
- Self- and peer-assessment opportunities.

Assessment is monitored by the Computing Lead to ensure consistent progression across year groups.

7. Resources and Access

The schools provides a broad range of hardware and software to support the Computing curriculum:

- Networked computers in Computer Suite and Chromebooks in classrooms;
- Interactive whiteboards and visualisers to enhance teaching;
- A range of licensed software and secure online platforms (including Kapow and LGfL resources).

7.1 Management of Resources

- The ICT Technician maintains all devices and ensures regular software and security updates.
- The Computing Lead liaises with the technician to audit and plan for resource renewal.
- Digital tools are selected based on their educational value, accessibility and compliance with data-protection requirements.
- The Federation uses LGfL as its Internet Service Provider and maintains appropriate filtering and monitoring arrangements in line with current Department for Education requirements and the school's safeguarding responsibilitie
- All staff and pupils use personal login credentials and secure storage for digital work.

7.2 Accessibility and Inclusion

- Access to Computing resources is equitable for all pupils.

  Assistive technologies (for example, text-to-speech, dictation, enlarged display and accessibility settings) are available to ensure full participation.
- Classrooms are organised so that technology is readily available and integrated naturally into learning.

8. Roles and Responsibilities

8.1 The Governing Board

The governing board:

- Has overall responsibility for monitoring this policy and holding the Executive Headteacher to account for its implementation. The governing board will ensure online safety is a running and interrelated theme in the whole-school approach to safeguarding and related policies and procedures, including when planning the curriculum, teacher training, the role of the DSL (and deputies) and any parental engagement
- Will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring
- Will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children
- Will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL)
- Will make sure that the schools teach pupils how to keep themselves and others safe, including online
- Will make sure that the schools have appropriate filtering and monitoring systems in place on school devices and school networks, and that a review of the effectiveness of the filtering and monitoring systems is carried out by SLT at least once every academic year. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the schools in meeting the standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
    - Reviewing filtering and monitoring provisions at least annually
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
    - Having effective monitoring strategies in place that meet the schools' safeguarding needs
- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the schools' ICT systems and the internet
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

8.2 Executive Headteacher, Heads of School and Senior Leadership Team (SLT)

- Ensure compliance with KCSIE, the Department for Education's current Filtering and Monitoring Standards, and relevant data-protection legislation.
- Provide staff training and monitor funding for Computing development
- Monitor policy implementation and report annually to governors
- Promote the safe and effective use of technology across the curriculum.

The Executive Headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the schools.

They will make sure that there are robust cover arrangements for when the DSL is unavailable due to illness, leave or other circumstances.

8.3 The Designated Safeguarding Lead (DSL)

Details of the schools' designated safeguarding leads (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Executive Headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the schools
- Working with the Executive Headteacher and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT technician/manager to make sure the appropriate systems and processes are in place
- Working with the Executive Headteacher, ICT technician/manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the schools' child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety

.

- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Executive Headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- Oversee all online-safety matters within the schools
- Ensure that staff understand how to identify and respond to online-safety incidents
- Liaise with external agencies and parents where required
- Review online-safety training annually

8.4 Federation Computing Lead

- Lead the implementation of the Kapow Primary Computing Scheme across both schools
- Support staff in planning, teaching and assessment
- Monitor standards through lesson visits, pupil voice and work sampling
- Coordinate staff training and maintain awareness of new technologies
- Work alongside the DSL to ensure online safety is integrated into all teaching
- Ensure consistency of provision and progression across the federation
- Coordinate resource sharing and joint procurement where appropriate
- Lead federation-wide computing initiatives and events

8.5 Class Teachers

- Deliver Computing lessons following the schools' scheme of work
- Model safe and responsible use of technology
- Adapt lessons to meet the needs of all pupils
- Maintain Computing books and digital portfolios as evidence of progress
- Reinforce online-safety messages in all digital activities

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the schools' ICT systems and the internet, and making sure that pupils follow the schools' terms on acceptable use

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes
- Working with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

8.6 ICT Technician/ICT Manager

- Maintain reliable, secure and up-to-date systems
- Ensure filtering and monitoring remain effective
- Respond promptly to technical issues and support staff in troubleshooting
- Advise the SLT and Computing Lead on resource needs and software updates

The ICT technician/manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the schools' ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the schools' ICT systems regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

8.7 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the Executive Headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the schools' ICT systems and internet

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

8.8 Visitors and Members of the Community

Visitors and members of the community who use the schools' ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use

9. Planning, Monitoring and Evaluation

Planning

- Teachers plan Computing lessons using the Kapow Primary Computing Scheme.
- Curriculum maps and plans outline the units of work, key vocabulary, and links to the National Curriculum and online-safety strands.
- Teachers adapt Kapow lesson materials to meet the needs of their classes and to make meaningful cross-curricular links.
- Computing is planned to ensure clear progression of skills and knowledge from EYFS through to Year 6.
- Long-term and medium-term plans are reviewed annually by the Computing Lead in consultation with staff and senior leaders.

Monitoring

The Computing Lead, supported by the Senior Leadership Team (SLT), monitors Computing provision through:

- Lesson observations and learning walks;
- Review of Computing books and (where needed and relevant) digital portfolios;
- Discussions with pupils and staff;

- Audits of resources and staff confidence;
- Analysis of assessment information from the Kapow progression framework.

Monitoring ensures that Computing teaching remains consistent, high quality and aligned with school improvement priorities.

Evaluation

Evaluation of the Computing curriculum focuses on:

- Pupil achievement and engagement;
- Staff feedback and training needs;
- Effectiveness of resources and technologies in use;
- Impact of online-safety teaching on pupil awareness and behaviour;
- Compliance with DfE and statutory safeguarding requirements.

Findings from evaluation inform the Computing Priorities.

10. Inclusion and Equal Opportunities

At St Charles and St Mary's, all pupils are entitled to high-quality Computing education and equal access to technology.

Inclusive Practice

- Lessons are adapted to meet the varying abilities and learning needs of pupils.
- Teachers use a range of approaches, grouping strategies and support to ensure full participation.
- Pupils with Special Educational Needs and Disabilities (SEND) receive additional support through adapted resources and assistive technologies.
- Gifted and talented pupils are provided with enrichment tasks and extension challenges
- Teaching reflects diverse perspectives and contributions in technology and innovation.

Equality and Accessibility

The schools are committed to ensuring that all learners, regardless of background or gender, have equal access to digital tools, resources and learning opportunities.

Computing contributes to promoting equality by encouraging collaboration, problem-solving and respect for others' ideas.

Resources and learning materials are selected to represent a diverse range of people, cultures and communities.

Accessibility in Practice

- Hardware and software are chosen for accessibility and usability.
- Visual, auditory and motor needs are considered when setting up devices.
- Support staff are trained to assist pupils effectively during Computing lessons.
- Accessibility features (such as speech-to-text, font enlargement and colour contrast) are enabled where needed.

Through inclusive teaching, every pupil at St Charles and St Mary's can access and enjoy Computing, develop confidence in their skills, and understand how technology can empower and include all members of society.
.

11. Internet Access and Online Safety

St Charles and St Mary's Catholic Primary Schools recognise that the internet is an essential element in education, business and social interaction.

The schools provide pupils with opportunities to access the internet and digital technologies safely, responsibly and purposefully, as part of their wider learning.

Teaching Online Safety

Online safety is taught as an integral part of the Computing curriculum through the Kapow Primary Computing Scheme and reinforced in PSHE and RSE lessons, as well as during assemblies and themed events such as Safer Internet Day.

Pupils are taught to:

- Use technology safely, respectfully and responsibly;
- Recognise acceptable and unacceptable online behaviour;
- Protect personal information and privacy;
- Report concerns or inappropriate content to trusted adults;
- Question the reliability of digital content and sources.

These lessons are age-appropriate, interactive and linked to real-life scenarios, helping pupils understand both the opportunities and risks of the online world

Internet Use

- Pupils access the internet for educational purposes and under appropriate staff supervision.
- Filtering and monitoring systems are maintained in accordance with KCSIE 2026 and the DfE's current Filtering and Monitoring Standards.
- Staff should consider the suitability of websites, applications and online content before using them with pupils.
- Staff and pupils follow the relevant Acceptable Use Policy, setting clear expectations for safe, respectful and responsible behaviour online.
- Breaches of acceptable use are managed in line with the school's Behaviour, Safeguarding and other relevant policies.
  Serious breaches, safeguarding concerns or concerns identified through filtering and monitoring are reported to the DSL and recorded through the school's safeguarding systems where appropriate.

School Website and Digital Communication

- The school website is managed by authorised staff under the direction of the Executive Headteacher and complies with statutory publication requirements.
- Photographs or videos of pupils are only used where parental consent has been obtained.
- Personal information such as full names and addresses are never published online.
- Email and communication tools are used respectfully and appropriately, with pupils using school-approved platforms only.

Social Media

Staff, pupils and parents are expected to use social media responsibly.

The schools do not permit unauthorised social media accounts representing either St Charles or St Mary's. Staff must not post content or images relating to pupils, colleagues or school activities on personal accounts. All communication with pupils and families should take place through official school channels.

.

12. Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the curriculum. They will also have Relationships Education and Health Education lessons.

In Key Stage (KS1), pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage (KS2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content By

the end of primary school, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites, which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel

.

worried or concerned about something they have seen or engaged with online

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

13. Practical Cyber Security Skills

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The physical security of devices
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber-incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

14. Educating Parents/Carers About Online Safety

The schools will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our websites.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Executive Headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the Executive Headteacher.

15. Cyber-bullying

15.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

15.2 Preventing and Addressing Cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The schools will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The schools may also send information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the schools will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the schools will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

Staff should be aware that children can experience harm from their peers online through:

- Unkind, threatening or hurtful messages
- Pressure to share personal information or images
- Being excluded from online groups or games
- Sharing of inappropriate images or content
- Behaviour online that makes others feel uncomfortable, unsafe or upset

In primary schools, peer-on-peer abuse online most commonly includes:

- Cyberbullying through messaging apps or gaming platforms
- Sharing embarrassing photos or videos without permission
- Spreading rumours or unkind comments
- Pressuring others to do things they're uncomfortable with online

While less common in primary settings, staff should also be aware that older primary pupils may:

- Be exposed to or share age-inappropriate content, including images generated or altered using AI
- Experience or perpetrate more serious forms of online abuse

All incidents of peer-on-peer abuse, whether online or offline, will be taken seriously and managed in line with our Child Protection and Safeguarding Policy and Behaviour Policy. Staff will respond with appropriate support for both the child who has been harmed and the child displaying harmful behaviour.

16. Artificial Intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes' or 'deep nudes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. We will treat any use of AI to bully pupils very seriously, in line with our behaviour policy.

Use of Artificial Intelligence

The Federation has a separate Artificial Intelligence (AI) Policy, which sets out the requirements for the safe, ethical and responsible use of AI across both schools.

Staff and governors must only use AI tools approved by the Federation and must follow the data protection, safeguarding and acceptable-use requirements set out in the Federation AI Policy. Personal, sensitive or confidential information must not be entered into open generative AI tools.

Pupils may only use AI tools where their use has been approved by the Federation, is appropriate for their age and educational purpose, and is appropriately supervised by staff.

All use of AI should protect pupils' privacy and personal data and comply with the Federation's Data Protection Policy and safeguarding procedures.

Full guidance, including approved AI tools, pupil access, staff responsibilities and data-protection requirements, is contained within the Federation Artificial Intelligence (AI) Policy.

17. Acceptable Use of the Internet in School

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the schools' ICT systems and the internet.

Visitors will be expected to read and agree to the schools' terms on acceptable use, if relevant.

Use of the schools' internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

18. Pupils Using Mobile Devices in School

The federation has a separate Mobile Phone Policy which sets out the rules and expectations for pupils, staff and visitors regarding the use of mobile phones and smart technology on school premises.

In line with statutory guidance and our Mobile Phone Policy, both schools operate as mobile phone-free environments during the school day to ensure pupils remain focused on their learning and social interactions, free from the distractions and potential risks associated with mobile phone use.

For full details, please refer to the Federation Mobile Phone Policy.

19. How the School Will Respond to Issues of Misuse

Where a pupil misuses the schools' ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the schools' ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The schools will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

20. Training for Staff, Governors and Volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

21. Data Protection and GDPR

St Charles and St Mary's Catholic Primary Schools comply fully with the UK General Data Protection Regulation (GDPR), the Data Protection Act (2018) and the Data (Use and Access) Act 2025, together with relevant guidance from the Information Commissioner's Office and Department for Education.

- All staff receive training on data protection and secure handling of personal information.
- Personal data, including pupil information and digital work, is stored securely within the school network or approved cloud platforms.
- Portable devices and storage media are password-protected.
- Staff only use school email accounts for professional purposes.
- Digital data is retained and deleted in accordance with the school's Data Protection Policy and retention schedule.
- Any data breaches are reported immediately to the Data Protection Officer (DPO) and managed following statutory procedures.

The school's data-handling practices reflect the Catholic ethos of respect for the dignity and privacy of every individual.

22. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety.This policy will be reviewed every year by the Governing Body. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

23. Links with Other Policies

This policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policies
- Staff disciplinary procedures
- Data protection policies and privacy notices
- Complaints procedure
- Mobile phones policy
- Federation Artificial Intelligence (AI) Policy

Associated Documents

The following associated documents support the implementation of this policy and are maintained separately by the Federation:

- Staff Acceptable Use Policy/Agreement
- Pupil Acceptable Use Policy/Agreement
- Relevant parental consent forms
- Data protection procedures

These documents are kept under review and are available to relevant staff, pupils, parents/carers and other stakeholders as appropriate.