St Mary's Catholic School
E-safety policy

Aims

This policy aims to help individuals understand their roles and responsibilities in ensuring the safe and acceptable handling/use of information technologies.

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, visitors and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2025, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying
- cyber-bullying: advice for Headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Applicable to all users of technology and connected systems:

Unlawful/inappropriate material must not be viewed/stored/distributed on any school system. This can include material which is in violation of any law/regulation or which can be considered by any reasonable person in its context to;

- be defamatory
- be violent
- be offensive
- be abusive
- be indecent or obscene
- be discriminatory
- incite hatred
- constitute bullying and/or harassment
- breach anyone's confidence, privacy, trade secrets or copyright

Roles and responsibilities

The governing body

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing body safeguarding link will co-ordinate regular meetings with the designated safeguarding leads (DSLs) to discuss online safety, and monitor online safety logs as provided by the designated safeguarding leads.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Leads

Details of the school's DSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT 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 school child protection policy
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMs 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 Headteacher and to the governing board

This list is not intended to be exhaustive.

The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's 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 school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

All staff

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 school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

- Working with the DSLs to ensure that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring 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'

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of the Senior Leadership Team or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

General guidelines for staff

- If someone has stated that they do not wish to receive emails from you then you must refrain from sending further e-mails to them. You must not use an organisation's email systems for 'spamming' purposes (the use of email to send unwanted/junk/advertising content to multiple recipients).
- Particular care should be taken whenever you choose to use your own personal technologies in a work environment and ensure that other people, including children, are not able to see personal contents which you would deem private or sensitive.
- You must ensure that your work/school computer account is not misused so you should not share your username or password with anyone. All Internet and network use of systems may be subject to monitoring by school and this may be traced back to you. Everyone is responsible for ensuring information systems are secure, safe and used to benefit all. You should be aware that disciplinary/civil/criminal action might arise if any user is found to be deliberately accessing material described above. Similarly, unauthorised or deliberate illegal access to or use of data, systems or networks is prohibited and may also result in disciplinary/civil/criminal action.
- Further information and guidance can be found in the Staff Code of conduct.

Educating students about online safety

Students will be taught about online safety as part of the Personal Development Programme. All students in Years 7 to 13 study a 'Staying safe online and offline' module.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including 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.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. We will continue to deliver safeguarding information evenings for parents both remotely and in person.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Head of Year.

Cyber-bullying

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Anti-bullying policy.)

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 are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff will have opportunities to use aspects of the curriculum to cover cyber-bullying. This includes the Personal Development Programme 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 school also sends information/leaflets on cyber-bullying to parents so that 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 school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.
Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (BBCET Acceptable Use Policy). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
Use of the school's 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 students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
More information is set out in the acceptable use agreements.

Students using mobile devices in school

Mobile phones are allowed to be brought to school by our students, although we recommend that they are not. Mobile phones and personally-owned mobile devices brought into school are the responsibility of the device owner. The School accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

• A student's phone must be switched off and kept in their inside blazer pocket, bag or locker unless a member of staff has given an instruction to do otherwise.
• Students are not allowed to use any phone during the School day (e.g. texting, photography, internet usage) unless a member of staff has given permission.
• A student is not allowed to contact anyone via phone call, text, social networking or email during the School day. This includes Parents/Guardians. Students may contact Parents/Guardians, in the case of an emergency, by using a phone in the School Office.
• Parents/Guardians are also not allowed to contact their child on a mobile device during the School day. Any message during the School day needs to go through the School Office.
• Breaches of these rules will lead to confiscation* of the phone.
The confiscated phone will be given to the student's Head of Year and will be returned the student at the end of the school day. It will be logged and kept in a safe until this time.
• In certain lessons (e.g. PE & Technology) it is the responsibility of the student to store their mobile phone in the safe area provided by the teacher.

The school's mobile phone policy is fully complaint with the Department for Education's 'Mobile phones in schools' guidance, published by the UK Government in February 2024.

Personal music systems
Personal music systems, of any type, must not be listened to during the School day, unless directed by a member of staff. Headphones must not be worn at any time. Any student seen to be wearing headphones will have the device confiscated and returned to the student at the end of the day.

Photography and Video and other electronic devices
Students are forbidden to use photography or video unless directed to by a member of staff. 'Smart watches' (e.g. Apple watch) are not allowed in school. Recording or taking pictures of a member of staff or another student by a student without permission will be taken extremely seriously and depending on the circumstances may result in exclusion. *These confiscations are allowed under governmental advice ref:
https://www.gov.uk/government/publications/searching-screening-and-confiscation

Staff using work devices outside school
All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in the acceptable use agreement. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

How the school will respond to issues of misuse
Where a pupil misuses the school's 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 school's 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 and staff code of conduct policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

Training
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, staff briefing and staff meetings).
- We will ensure that all staff receive online safety training as part of induction and that ongoing online safety training and updates for all staff will be integrated, aligned and considered as part of our overarching safeguarding approach. Amongst other things, this includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

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

- Children can abuse their peers online through:
- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

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 the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSLs 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.

Monitoring arrangements

The DSLs and Pastoral Staff log behaviour and safeguarding issues related to online safety on CPOMs.

This policy will be reviewed every year by the Headteacher. 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.

Information system security

- The School's ICT system capacity and security will be reviewed.
- Virus protection is installed and updated regularly.
- Security strategies will be discussed with the LA and implemented to ensure best practice is maintained.
- Unapproved system programs, utilities and executable files will not be allowed in students' work areas or attached to e-mail.

E-mail

- Students will be encouraged to use approved e-mail accounts on the school system, the use of personal web mail accounts such as Hotmail may be blocked as appropriate.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be in a professional manner.
- The forwarding of chain letters is not permitted.

Microsoft Teams

Microsoft Teams is used in school for teaching and learning, for setting homework and for the sharing of notices and information. Students and staff also have the availability to use the messaging facility to share information or to access additional support if needed. All communication on Microsoft Teams should be professional and appropriate. Any misuse of Teams will be dealt with in line with the school's behaviour policy. Further information for staff can be found in the staff code of conduct.

Published content and the school web site

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or students personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected with children's safety in mind.
- Students' full names will not be used anywhere on the Web site without express permission.
- Written permission from parents will be obtained before photographs of students and/or full names are published on the school Web site or any other medium.
- When publishing students' work, staff must take care to ensure that no personal information is revealed in the work that can be connected to a student.

Social networking and personal publishing

- School will block/filter access to social networking sites wherever possible.
- Newsgroups will be blocked, where possible, if they contain inappropriate material.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students will be advised not place inappropriate photos or personal details on any social network space and made aware of the security implications of this.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications.

Appropriate filtering and monitoring

The leadership and relevant staff are:

- Aware of all internet monitoring and filtering systems
- Manage them effectively
- Know how to escalate concerns when they are identified

We will do all we reasonably can to limit children's exposure to online risks through school provided IT systems and will ensure that appropriate filtering and monitoring systems are in place. Settings should list details of how this is established and achieved e.g. which filtering and monitoring systems or approaches are in place and why these decisions have been made. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards.

If children or staff discover unsuitable sites or material, they are required to turn off monitor / screen and report the concern immediately to a member of staff, who will report the URL of the site to technical staff / services. All users will be informed that use of our systems can be monitored, and that monitoring will be in line with data protection, human rights, and privacy legislation. Filtering breaches or concerns identified through our monitoring approaches will be recorded and reported to the DSL who will respond as appropriate. Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the Internet Watch Foundation and the police.

When implementing appropriate filtering and monitoring, we will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

We acknowledge that whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of our approach to online safety. Children will use appropriate search tools, apps and online resources as identified following an informed risk assessment. Children's internet use will be supervised by staff according to their age and ability. Children will be directed to use age appropriate online resources and tools by staff.

While the school makes every effort to protect students from unsuitable materials, due to the international scale and connected nature of Internet content, it is impossible to guarantee that unsuitable material will never appear on a school computer. Filtering is carried out by both the LA and the school (Smoothwall). The school will work in partnership with the LA, BBCET, DfE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.

If staff or students discover an unsuitable site, it must be reported to the ICT Manager and DSL.

Regular checks are made to ensure that the filtering methods selected are appropriate and reasonable.

The use of "proxy sites" to bypass school or LA filters is prohibited and the school will endeavour to block these.

Managing videoconferencing and filming/photography

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Videoconferencing will be appropriately supervised for the students' age.
- Parents and carers should agree for their children to take part in videoconferences, filming or photography, in the annual data collection sheet at the start of the academic year.
- Personal recording equipment, cameras and mobile phones must not be used in school without permission from the class teacher.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones of students must be switched off and out of sight at all times in school.
- Staff should not provide their mobile phone number to parents or students. A school contact mobile number is available for all visits.
- In exceptional circumstances, such as school trips, staff can be provided with a mobile phone for use.

Assessing risks

- **Protecting personal data** will be recorded, processed, made available according to Data Protection Act 1998.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor NCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Links with other policies

This E-safety policy is linked to our:

- BBCET Safeguarding and Child Protection policy
- Behaviour policy
- Staff disciplinary procedures
- BBCET Data protection policy and privacy notices
- BBCET Complaints policy
- BBCET Acceptable use policy

Policy review date	**By whom**	**Approved** *(insert date)*
September 2025	Local Governing Committee	10th October 2025