St Mary's Catholic College
Wallasey

Online Safety Policy 2026-2028

Date of publication: September 2026

Reviewed by: **Governing body**

Issued to: **All stakeholders (Website)**

Next review date: September 2027 (annual review; full renewal by September 2028)

WRITTEN BY:	Mr K Maddocks
HEADTEACHER	Mr K Maddocks
CHAIR OF GOVERNORS	Mrs R Clarke

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 4
4. Educating pupils about online safety 6
5. Educating parents about online safety 6
6. Cyber-bullying 7
7. Acceptable use of the internet in college 8
8. Pupils using mobile devices in college 8
9. Staff using work devices outside college 8
10. How the college will respond to issues of misuse 9
11. Training 9
12. Monitoring arrangements 10
13. Links to other policies 10

Appendix 1: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers) 11
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) 12

1. AIMS

Our college aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole college 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

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, antisemitism, 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; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education 2026 (KCSIE), and will be read alongside the latest version of that guidance.

It also takes account of the DfE's statutory guidance on mobile phones in schools (2026), the DfE filtering and monitoring core standard, Teaching online safety in schools, Relationships Education, Relationships and Sex Education and Health Education, Searching, screening and confiscation, and the Prevent duty guidance.

The policy reflects relevant legislation including, but not limited to, the Education Act 1996 (as amended), Education and Inspections Act 2006, Education Act 2011, Equality Act 2010, Children and Families Act 2014, UK GDPR and Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025, and the Online Safety Act 2023 where relevant.

The policy also takes account of the DfE's Generative AI: product safety standards and current DfE guidance on the safe and appropriate use of generative artificial intelligence in education.

It also takes into account the National Curriculum computing programmes of study.

Keeping Children Safe in Education

- 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 protecting children from radicalisation Education Act 1996, Education and Inspections Act 2006, Equality Act 2010, Education Act 2011.

3. ROLES AND RESPONSIBILITIES

3.1 The local governing body

The local governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The local governing body will coordinate regular meetings with appropriate staff to discuss online safety, and monitor CPOMS online safety logs as provided by the designated safeguarding lead (DSL).

The link governor who oversees online safety is the safeguarding link governor.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the college's ICT systems and the internet policy
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole college or college approach to safeguarding and related policies and/or procedures
- Ensure 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
- Ensure that appropriate filtering and monitoring systems are in place, that roles and responsibilities are clearly assigned, and that the provision is reviewed and documented at least annually in line with DfE standards.
- Ensure that online safety, including emerging risks from generative AI and AI-generated content, remains an interrelated theme within the school's safeguarding arrangements.

3.2 THE HEADTEACHER

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

3.3 THE DESIGNATED SAFEGUARDING LEAD

Details of the college's designated safeguarding lead (DSL), and deputy safeguarding leads, 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 college, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the college
- 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 college 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 and dealt with appropriately in line with the college behaviour policy and anti-bullying policy
- Updating and delivering staff training on online safety

- Liaising with other agencies and/or external services if necessary
- Providing termly DSL reports, to include issues around online safety, via the HFCMAT DSL safeguarding report.
- Taking lead responsibility for safeguarding and child protection matters identified through monitoring systems and ensuring appropriate action is taken and recorded.
- Working with IT support and senior leaders to review the safeguarding implications of new technology, including generative AI tools, before or during implementation.

This list is not intended to be exhaustive.

3.4 ICT MANAGEMENT

The Trust ICT infrastructure and college ICT manager, working with the DSL and senior leadership, are responsible for:

- Maintaining appropriate filtering and monitoring systems that protect users from illegal, inappropriate and potentially harmful content, including text, images, audio, video and AI-generated content.
- Ensuring that filtering and monitoring arrangements reflect the needs and risk profile of pupils and staff and do not unreasonably restrict teaching and learning.
- Supporting a documented review of filtering and monitoring provision at least once every academic year, involving senior leadership, the DSL, IT support and the responsible governor.
- Reviewing filtering and monitoring when safeguarding risks are identified, working practices change, new technology or generative AI tools are introduced, major software changes occur, or network/device configurations materially change.
- Keeping records of filtering and monitoring checks, actions and outcomes, and ensuring high-risk safeguarding alerts are escalated promptly to the DSL.
- Ensuring new school-managed devices and services are appropriately filtered and monitored before deployment and seeking assurance following significant system or equipment changes.
- Maintaining appropriate cyber-security controls, including patching, malware protection, account security and multi-factor authentication where required by Trust arrangements.
- Blocking access to illegal or inappropriate content while maintaining suitable differentiated access for staff and pupils.
- Ensuring online safety or cyber-bullying concerns identified through technical systems are reported promptly through the school's safeguarding and behaviour procedures.

This list is not intended to be exhaustive.

3.5 ALL STAFF AND VOLUNTEERS

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 college's ICT systems and the internet and ensuring that pupils follow the college's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are reported and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the college 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.

3.6 PARENTS

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child complies with the acceptable use of the college's ICT systems and internet
- Parents can seek further guidance on keeping children safe online from the following organisations and websites: https://www.childnet.com/help-and-advice/parents-and-carers , https://www.nspcc.org.uk/keeping-children-safe/online-safety/

3.7 VISITORS AND MEMBERS OF THE COMMUNITY

Visitors and members of the community who use the college'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.

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the ICT, Computing and the Inspire curriculum and the Relationships and sex education and health education in secondary schools

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 explicitly taught as part of the Inspire programme. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Pupils will also be taught, at an age-appropriate level, about generative AI and AI-generated content. This will include recognising that AI outputs can be inaccurate or misleading, protecting personal information, understanding appropriate and ethical use, recognising manipulated media and deepfakes, and knowing how to report harmful or concerning AI-generated content.

Where pupils use school-approved generative AI tools, this will be in accordance with age restrictions, school expectations, appropriate supervision and the school's filtering and monitoring arrangements.

5. EDUCATING PARENTS ABOUT ONLINE SAFETY

The college will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Google classroom this policy will also be shared with parents via the college website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the relevant year group team or DSL.

The college will, where appropriate, provide parents and carers with information about emerging online risks, including generative AI, deepfakes, online scams and changes in the use of social media and smart technology.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. CYBER-BULLYING

6.1 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the college behaviour policy and anti-bullying policy.)

6.2 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 are encouraged to do so, including where they are a witness rather than the victim.

The college will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This will be covered during Inspire time and in computing/ICT lessons.

This includes bullying, harassment, impersonation or sexualised abuse involving manipulated or AI-generated images, audio or video. Such incidents will be treated as safeguarding and/or behaviour concerns as 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 college 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 college will follow the processes set out in the college behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the college will use all reasonable endeavours to ensure the incident is contained. Such as contacting parents and social media companies.

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.

6.3 EXAMINING ELECTRONIC DEVICES

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or is identified in the college rules as a banned item for which a search can be carried out, and/or is evidence in relation to an offence

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation
- Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or undermine the safe environment of the college or disrupt teaching, and/or commit an offence
- If inappropriate material is found on the device, the DSL must be immediately alerted, who will decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
- When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:
- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or the pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance

on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the college complaints procedure.

7. ACCEPTABLE USE OF THE INTERNET IN COLLEGE

All pupils, parents, staff, volunteers and governors agree to the college's acceptable use of the ICT systems and the internet when they login in to the college system. Visitors will be expected to read and agree to the college's terms on acceptable use if relevant.

Use of the college'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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements found in appendix 1&2.

8. PUPILS USING MOBILE DEVICES IN COLLEGE

- Keeping operating systems up to date by always installing the latest updates
- Staff members must not use the device in any way which would violate the college's terms of acceptable use, as set out in appendix 2.
- Work devices must be used solely for work activities.
- Staff must not enter personal, special category, confidential or safeguarding information into generative AI tools unless the tool has been specifically approved for that purpose by the Trust/school and its data protection implications have been assessed.
- Staff using approved generative AI must exercise professional judgement, check outputs for accuracy, biIn line with statutory DfE guidance, St Mary's is a mobile phone-free environment throughout the school day for pupils in Years 7–11. This includes lessons, movement between lessons, breaktimes and lunchtime.

Pupils may bring a mobile phone to college for use when travelling to and from school, but it must be secured in accordance with the college's Yondr/mobile phone procedures on arrival and must not be accessed or used during the school day unless an authorised exception applies.

The school may apply sanctions, including confiscation, where the mobile phone policy is breached. Any searching, screening or confiscation will be undertaken in line with the school's Behaviour Policy and current DfE guidance.

Reasonable adjustments and individual arrangements will be made where required by law or where there is an evidenced medical, SEND, safeguarding or other exceptional need. Such access will be for an agreed purpose, time and location.

Any arrangements for Sixth Form students will be set out in the college's Behaviour/Mobile Phone Policy and will ensure that any permitted use is limited to designated times and locations and does not undermine the mobile phone-free environment for younger pupils.

9. STAFF USING WORK DEVICES OUTSIDE COLLEGE

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
- 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
- as, appropriateness and copyright/data-protection risks, and remain accountable for any material they use or share.
- Suspected phishing, compromised accounts, malware, data breaches or other cyber-security incidents must be reported promptly in accordance with Trust procedures.
- If staff have any concerns over the security of their device, they must seek advice from Hi-Impact IT helpdesk.

10. HOW THE COLLEGE WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the college's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and internet acceptable use policy 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 college'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/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. 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, 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
- 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 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.
- Training and updates will reflect emerging online safety risks, including developments in generative AI, deepfakes and manipulated media, online scams, filtering and monitoring, and relevant changes to statutory guidance.
- More information about safeguarding training is set out in our child protection and safeguarding policy.

12. MONITORING ARRANGEMENTS

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS.

This policy will be reviewed at least annually and updated sooner where there are significant changes to statutory guidance, technology, safeguarding risks or school practice. Following each review, the policy will be shared with the governing body. A full renewal is scheduled no later than September 2028.

.

13. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

APPENDIX 1: KS2, KS3 AND KS4 ACCEPTABLE USE AGREEMENT (PUPILS AND PARENTS/CARERS)

ACCEPTABLE USE OF THE COLLEGE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:
I will read and follow the rules in the acceptable use agreement policy. **When I use the college's ICT systems (like computers) and get onto the internet in college I will:** Always use the college's ICT systems and the internet responsibly and for educational purposes only Only use them when a teacher is present, or with a teacher's permission Keep my usernames and passwords safe and not share these with others Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others Always log off or shut down a computer when I've finished working on it **I will not:** Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity Open any attachments in emails, or follow any links in emails, without first checking with a teacher Use any inappropriate language when communicating online, including in emails Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate Log in to the college's network using someone else's details Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into college:** I will not use it during the college day **I agree that the college will monitor the websites I visit and that there will be consequences if I don't follow the rules.**
Signed (pupil): | **Date:**
Parent/carer's agreement: I agree that my child can use the college's ICT systems and internet when appropriately supervised by a member of college staff. I agree to the conditions set out above for pupils using the college's ICT systems and internet, and for using personal electronic devices in college, and will make sure my child understands these.
Signed (parent/carer): | **Date:**

Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE COLLEGE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the college's ICT systems and accessing the internet in college, or outside college on a work device (if applicable), I will not: Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) Use them in any way which could harm the college's reputation Access social networking sites or chat rooms Use any improper language when communicating online, including in emails or other messaging services Install any unauthorised software, or connect unauthorised hardware or devices to the college's network Share my password with others or log in to the college's network using someone else's details Take photographs of pupils without checking with teachers first Share confidential information about the college, its pupils or staff, or other members of the community Access, modify or share data I'm not authorised to access, modify or share Promote private businesses, unless that business is directly related to the college	
I will only use the college's ICT systems and access the internet in college, or outside college on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the college will monitor the websites I visit and my use of the college's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside college, and keep all data securely stored in accordance with this policy and the college's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the college's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**