Online safety policy

St. Michael's Catholic Grammar School

Approved by:	Ethos Committee	**Date:**	2nd October 2023
Last reviewed on:	N/A		
Next review due by:	Autumn 2025		

Contents

---

1. Aims

Our school 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 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

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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and 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 policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing body

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

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- 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

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's DSL and deputy 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 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 MyConcern 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 school behaviour policy

- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 IT Team

The IT Team is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, (NEW SYSTEM -Securly 2023) 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

  Web Filtering is provided via the new software Securly

  Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

  The school has a live subscription to Sophos Cloud Protection which provides defence against viruses and malware. This is updated automatically when the on device agent checks in with the cloud management console.

- Conducting a full security check and monitoring the school's ICT systems on a weekday basis

  Onsite IT carry out daily checks which cover the following;

  1. Check status of the backups (First thing every morning)
  2. Server room checks (Make sure A/C is working, no warning lights, no alarms – Daily)
  3. Prioritise/assign tickets to work on for the day
  4. Check extension for Voicemails – If anything needs to be logged/responded to urgently

  Outsourced IT – Proactive monitoring is configured and alerts relating to the servers, firewall and connectivity are investigated and resolved during working hours.

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

  Securly blocks the navigation to dangerous sites via categorisation and Sophos will assist in preventing the execution of dangerous file types.

- Ensuring that any online safety incidents are logged on MyConcern and dealt with appropriately in line with this policy

  This will be carried out via onsite IT after being notified of an incident in conjunction with a Safeguarding Officer.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

  Onsite IT will escalate any known incidents to the relevant Safeguarding Officer should they become aware of such incidents. Securly offer a bolt-on service (Securly Auditor) which would scan Gmail, Google Docs and Google Drive for instances of inappropriate content.

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 school's ICT systems and the Code of Conduct
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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.

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 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

3.7 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).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- 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)
- See Appendix 3 for School's curriculum

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.

5. 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.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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 school behaviour 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 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. Form tutors will discuss cyber-bullying with their tutor groups as part of the tutorial programme and Year 7 citizenship.

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 (see section 11 for more detail).

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.

6.3 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 pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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 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 in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

KS3 and Year 10 Pupils may bring mobile devices into school, but are not permitted to use them during school time:

Year 11 are permitted to use their mobile phone in their form room during breaktime and lunchtime

KS5 students may bring mobile devices or laptops into school and use the school wi-fi to help with their studies. They are not permitted to use the phone outside sixth form areas (Study room, form rooms, common room)

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1)

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. 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 appendix 3.

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 IT manager

10. 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 in Behaviour 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 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/staff code of conduct. 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.

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 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 DSL and deputy 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.

12. Monitoring arrangements

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

This policy will be reviewed every year by the Deputy Headteacher. At every review, the policy will be shared with the governing board. The review (such as the one available here) 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.

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

Appendix 1:

Name of pupil: Form:

I will read and follow the rules in the acceptable use agreement policy:

When I use the school's ICT systems, including the internet in school, I will:

- Only log-in using my own username and will not share my username with anyone else. I understand that I am responsible for the security of my own username and password.
- Always log-off or shut down a computer when I am working on it.
- 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.
- Always use the school's ICT systems and the internet responsibly and for educational purposes only.
- Tell a member of staff immediately if I find any material which is illegal or might upset, distress or harm me or others.
- Always use professional levels of language and content in my e-mails and Google Classroom message/comments.
- Check my e-mail account and Google Classrooms on a regularly for communication from staff.
- Only contact staff using private Google Classroom/e-mail when direct contact cannot be made (i.e. when education is remote).
- Make myself aware of the departmental policies for responding to queries received electronically (these policies can be found via Google Classrooms).
- Always be aware that the school may check my computer files, and monitor the websites/applications that I visit. I understand that my internet access at school can be withdrawn if any misuse is discovered.
- Never involve myself in cyber-bullying, whether at home or at school. I understand that making any comments/sending any messages/sharing any material that can cause hurt and upset to others will always be viewed by the school as cyber-bullying and treated as serious anti-social behaviour. I will always remember that I have a collective responsibility for the content of any group chats that I am a member of.

When I use the school's ICT systems, including the internet in school, I will not:

- Access any inappropriate websites including: social networking/media sites, chat rooms or gaming sites.
- Open any attachments in e-mails, or follow any links in e-mails, that I cannot identify. If I am unsure I will ask a member of staff.
- Use any inappropriate language (including swearing and discriminatory language) when communicating online, including in e-mails.
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.
- Post any anonymous comment or forward 'chain-letters'.
- Use the school's ICT systems for any personal financial game (including gambling) political purposes or advertising.

For Key Stage 5 students

When I bring a personal mobile device or any other personal electronic device (such as laptops or tablets) into school, and use the school WiFi, I will:

- Use my device responsibly, and will not access website or application that is not allowed when the using ICT systems.
- Recognise that I am solely responsible for my mobile phone/personal electronic device and that school bears no liability.

When I bring a personal mobile device or any other personal electronic device (such as laptops or tablets) into school, and use the school WiFi, I will not:

- Use my phone around the school site (except the Sixth Form Area), during lessons, tutor time, tutorials, clubs or any other activities without a teacher's permission.
- Take any photographs or record video/sound without a teacher's permission.

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school 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 school'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 school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, 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 school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school'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 school, and keep all data securely stored in accordance with this policy and the school'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 school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Computer science – Online safety

Year 7:

Social networking; covers aspects of online dangers such as cyberbullying, online strangers and inappropriate content. This allows the pupils to have the opportunity to identify ways of keeping themselves safer online; blocking users, protecting online identity and knowing ways of reporting incidents.

Online security; covers subject specific terminology such as spam(malware), phishing, viruses and analyse ways of protecting personal information. Pupils are able to justify ways of protecting confidential information online; consider approaches to downloading anti-virus software, managing unwanted emails on the internet and using secure passwords to shield their personal information.

Year 8:

Computer crime and security; covers aspects of legislation such as computer misuse and data protection. Students are able to analyse ways of hacking; the use of malware, phishing and brute force attacks (password protection). Pupils are given the opportunity to investigate computer crime and discover ways of acceptable behaviour on the internet. Data protection act enables pupils to understand the importance of unauthorised access, data harvesting tools and reflect upon sharing data or personal information on social media platforms. This creates an environment where students are able to identify harmful behaviour on the internet; bullying, grooming, assault or harassment and know the support systems available in place to help them report their concerns

Digital Citizenship Year 7

Scheme of Work Digital Citizenship

Respect Your Self/Respect Others
Digital Law

Lesson 1. School rules, Home rules, The Law

Swearing, posting images without permission, explicit photos, cyber-bullying, bringing school and teachers and others into disrepute. Being unkind to people, leaving people out. **Resources -** School Internet agreement.

Lesson 2. Images **Resources** PPT trust me – content. Personal information, Safer Internet ppt2017

Educate Your Self/Connect with Others
Digital Commerce

Lesson 3. Social media, types, age, privacy settings **Resources** Social media quiz, PPT contact2

Lesson 4. Using internet buying, information and images online, fake news- Be a critical analyser of information. Propaganda **Resources** Propaganda ppt

Protect Your Self/Protect Others
Digital Health and Welfare

Lesson 5. Know how to protect yourself Video – Consequences (Youtube)

Lesson 6. Mental Health/Physical health and the Internet. Human Brain is a social thing. It thrives on interaction with other brains. Social interaction with others in real life is necessary for good mental health. Distracted by phones when walking/crossing the road. Expensive careful of thieves. Discussion and making a poster.

https://www.**saferinternet**.org.uk

http://www.childline.org.uk/pages/home.aspx

CEOP - Official Site

https://www.thinkuknow.co.uk/

KS3 Tutorials

Year 7 look at mobile phone addiction in the Autumn term and look at Bullying online as part of 2 tutorials on bullying in the Spring Term

Year 8 have 2 lessons on Cyberbullying and internet safety in the Spring Term

All KS3 had either an assembly or tutorial on Peer on Peer abuse where it was highlighted that this could happen online.

KS4 Tutorials

- Internet Safety- general, how to protect onlineprivacy, identity, consequences
- The Dark Web
- Sexting, law, effects
- Revenge Porn
- Pornography

Yr 10 EL lessons

- Online sexual bullying, abuse, harassment, where to get help

KS5 Tutorials

- Sexting: The law and how to protect yourself
- Online violent extremism