EMMAUS
CATHOLIC MAC

Online Safety Policy

Version	6.0
Date created/updated	August 2026
Ratified by	Full Board
Date ratified	26th August 2026
Date issued	August 2026
Policy review date	August 2027
Post holder responsible	School Improvement/Inclusion Leads

Commitment to Equality:

We are committed to providing a positive working environment which is free from prejudice and unlawful discrimination and any form of harassment, bullying or victimisation. We have developed a number of key policies to ensure that the principles of Catholic Social Teaching in relation to human dignity and dignity in work become embedded into every aspect of school life and these policies are reviewed regularly in this regard.

This Online Safety Policy has been approved and adopted by Emmaus Catholic Multi Academy Company on 26th August 2026 and will be reviewed in August 2027 or sooner in line with any statutory changes.

Signed by Director of Emmaus Catholic MAC: J Griffin

Signed by CEO for Central Team: S Horan

This policy relates to all Emmaus schools and settings.

Mission
Forming Christ-centred pilgrims of hope with kind hearts, questioning minds, a thirst for knowledge and a hunger for justice.

Section	Changes
Legal Framework	Updated statutory guidance dates for KCSIE (2026), filtering and monitoring standards, and generative AI guidance.
Roles and Responsibilities	Clarified staff requirements to read Part One of KCSIE 2026 in full, assigned a named SLT member to filtering and monitoring oversight, and integrated filtering and monitoring responsibilities into the DSL's statutory job description.
Managing Online Safety & Risks	Added explicit definitions and references covering AI-generated deepfakes, digitally altered intimate imagery, and heightened focus on tackling misogyny and sexualised harassment.
Online Safety Training & Curriculum	Integrated AI deepfakes and emerging tech risks into curriculum coverage and staff safeguarding training expectations.
Generative Artificial Intelligence (AI)	Aligned AI safety measures and risk assessment expectations directly with DfE generative AI product safety expectations.
Acceptable Use Agreements (Appendices)	Updated pupil and staff agreements to explicitly prohibit generating, editing, or sharing AI-altered or deepfake nude/semi-nude imagery.

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. Managing online safety
4. Cyberbullying
5. Child-on-child sexual abuse and harassment
6. Grooming and exploitation
7. Mental health
8. Online hoaxes and harmful online challenges
9. Cyber-crime
10. Online safety training for staff
11. Online safety and the curriculum
12. Use of technology in the classroom
13. Use of smart technology
14. Educating parents
15. Internet access
16. Filtering and monitoring online activity
17. Network security
18. Emails
19. Generative artificial intelligence (AI)
20. Social networking
21. The school website
22. Use of devices
23. Remote learning
24. Monitoring and review

Statement of intent

Emmaus Catholic Multi Academy Company '(The MAC)' understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, for example:
    - Pornography.
    - Racism.
    - Misogyny.
    - Self-harm.
    - Suicide.
    - Discrimination.
    - Radicalisation.
    - Extremism.
    - Misinformation.
    - Disinformation, including fake news.
    - Conspiracy theories.
- **Contact**: Being subjected to harmful online interaction with other users, for example:
    - Peer to peer pressure.
    - Commercial advertising.
    - Adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, for example:
    - Making, sending and receiving explicit messages.
    - Consensual and non-consensual sharing of nudes and semi-nudes, including digitally altered images, deepfakes, and AI-generated intimate imagery.
    - Sharing of pornography.
    - Sharing other explicit images.
    - Online bullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils, and staff will revolve around these areas of risk.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2026) 'Filtering and monitoring standards for schools and colleges''
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2026) 'Keeping children safe in education 2026' (KCSIE) DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2026) 'Generative artificial intelligence in education' Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated March 2024)'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies (Amend these as appropriate to your school):

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Pupils' Personal Electronic Devices Policy
- Staff Code of Conduct
- Behaviour Policy

- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy
- Photography and Images Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy
- Remote Education Policy
- Safe Use of AI Policy

Roles and responsibilities

The Local Governing Body will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSLs remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including reading Part One of KCSIE 2026 in full) at induction and at regular intervals, covering filtering and monitoring expectations, emerging AI risks, and online safety.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least once every academic year by the designated SLT member responsible for filtering and monitoring, in liaison with the DSL and IT support, with written records of checks maintained. Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.

The principal will be responsible for:

- Ensuring that online safety is a running an interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and Local Governing Body to update this policy on an annual basis.

Assigning a designated member of the Senior Leadership Team (SLT) to hold overall leadership responsibility for the school's filtering and monitoring systems, supported by the DSL and IT staff. The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety, maintain explicit responsibility for filtering and monitoring systems in their job description, and recognise additional risks that pupils with SEND face online. Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Providing specialist knowledge in relation to filtering system management, e.g. the content and websites pupils should and should not be able to access.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.

- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Reporting to the Local Governing Body about online safety on a termly basis.
- Working with the Principal and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the Principal and Local Governing Body to update this policy on an annual basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the principal.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and Principal to conduct half-termly light-touch reviews of this policy.
- Providing specialist support in relation to the implementation of filtering and monitoring software.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.

- Reporting online safety incidents and concerns in line with the procedures within this policy.

Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the Principal where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular cyber security training, covering a range of topics including online safety.
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted termly on the topic of remaining safe online

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the principal, who decides on the best course of action in line with the relevant policies. If the concern is about the principal, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the principal and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the principal contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse

Discriminatory bullying online, misogyny, harassment, and harmful gender-based or sexualised behaviour. The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, generating, altering, or distributing nude or semi-nude imagery of other children (including AI-generated images and deepfakes) is a safeguarding concern and criminal offence, regardless of consent, depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the safeguarding policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been

manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the schools Prevent Duties.

Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Special Educational Needs and Disabilities (SEND) Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an "**online hoax**" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, "**harmful online challenges**" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the principal will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.

- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and principal will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and principal will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Computing
- Relationships and health education
- PSHE

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online will always be considered when developing the curriculum.

The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content Risks

Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as pornography, racism, misogyny, AI-generated deepfakes, self-harm, suicide, anti-Semitism,

radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Contact Risks

The school will educate pupils about the potential dangers of interacting with others online. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct Risks

Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with creating, sharing, or receiving explicit images, including both consensual and non-consensual exchanges of nudes and semi-nudes. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce Risks

The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The principal and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering

from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Desktop computers
- Laptops
- Tablets
- Internet and Intranet access
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the school's Acceptable Use Agreement for Staff.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom.

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.

- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Year Group Curriculum Meeting and Handbook
- Parents' evenings
- Newsletters
- Online resources

Internet access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the school office.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

Filtering and monitoring online activity

The Local Governing Body will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The Local Governing Body will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The principal and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems will be scaled appropriately to meet the safeguarding needs of all pupils. ICT technicians will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the principal. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

All staff will receive regular training on the operation and purpose of filtering and monitoring systems, including their role in safeguarding.

Personal devices connected to the school's network will be subject to the same filtering and monitoring standards to ensure consistent safeguarding measures.

Filtering and monitoring systems will undergo at least an annual review to assess their effectiveness and relevance.

Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the principal will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

The DSL will be responsible for implementing appropriate network security measures in liaison with the DPO and IT. Full details of the school's network security measures can be found in the Cyber Security Policy.

Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Pupil Confidentiality Policy and Staff and Volunteer Confidentiality.

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. School SLT annual assembly where they explain what a phishing email and other malicious emails might look like – this assembly will include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

Generative artificial intelligence (AI)

When deciding whether to use generative AI, safety will be the top priority. Any use of AI tools by staff and pupils will be carefully considered and assessed, evaluating the benefits and risks of its use in the school.

AI tools will only be used in situations where there are specified clear benefits that outweigh the risks, e.g. where it can reduce teacher workload, and the school will ensure that any use of AI tools comply with wider statutory obligations, including those outlined in KCSIE.

The school will carry out an AI Risk Assessment, which includes plans for mitigating against unauthorised use cases.

Pupils will only be permitted to use generative AI in the school with appropriate safeguards in place, e.g. close supervision and the use of tools with appropriate filtering and monitoring features in place.

For any use of AI, the school will:

- Comply with age restrictions set by AI tools and open access large language models (LLMs).

- Consider online safety, including AI, when creating and implementing the school's approach to safeguarding and related policies and procedures.
- Consult KCSIE to ensure all statutory safeguarding obligations and AI tools are used safely and appropriately.

Refer to the DfE's 'Generative AI: product safety expectations' alongside the DfE filtering and monitoring standards to ensure safeguards cover AI tools. The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupils' ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

The school will introduce a comprehensive AI Policy that clearly defines how AI technologies will be utilised responsibly and securely. This policy will outline the potential risks associated with misuse, as well as the safeguarding measures the school will implement to ensure the safe and ethical application of AI tools

Social networking

The use of social media by staff and pupils will be managed in line with the school's code of conduct.

The school website

The principal will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Device User Agreement.

The use of personal devices on the school premises and for the purposes of schoolwork will be managed in line with the Staff code of conduct.

Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the principal conduct half-termly light-touch reviews of this policy to evaluate its effectiveness.

The Local Governing Body, Principal and DSL will review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is August 2026.

Any changes made to this policy are communicated to all members of the school community.

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE MAC/SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the MAC/school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends. This includes anything another child does online that makes me feel worried or unsafe.
• Use MAC/school computers for school work only
• Be kind to others online, including not sending unkind messages or sharing pictures of others without permission.
• Look after the MAC/school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• I will not send, share or ask for photos or videos that could upset others.
• Log off or shut down a computer when I have finished using it
I agree that the MAC/school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the MAC/school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the MAC/school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE MAC/SCHOOL'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 MAC/school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the MAC/school'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 • Take, share, request, generate, or store nude or semi-nude images or videos of anyone, including images that have been created, edited, or altered using apps, generative AI, or deepfake tools Log in to the MAC/school'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 school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the MAC/school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the MAC/school will monitor the websites I visit and that there will be consequences if I don't follow the rules. I understand that unsafe online behaviour may result in safeguarding action, not just school sanctions.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the MAC/school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the MAC/school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, directors, governors, volunteers and visitors)

ACCEPTABLE USE OF THE MAC/SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/director/governor/volunteer/visitor:	
When using the MAC/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 MAC'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 MAC/ school's network • Share my password with others or log in to the MAC/school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the MAC/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 MAC/school	
I will only use the MAC/school's ICT systems and access the internet in MAC, or outside the MAC on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the MAC/school will monitor the websites I visit and my use of the MAC/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 MAC/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 understand the school's filtering and monitoring systems and will report concerns where I believe these may not be effective. I will remain vigilant to emerging online risks, including AI-generated content and online peer-on-peer abuse. I will always use the MAC/school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/director/governor/volunteer/visitor):	**Date:**

Appendix 4: Online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the MAC/school's acceptable use agreement for staff, directors, volunteers, governors and visitors?	
Are you familiar with the MAC/school's acceptable use agreement for pupils and parents/carers?	
Do you understand the school's filtering and monitoring systems and how to report concerns about their effectiveness?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Are you confident in recognising and responding to emerging online risks, including AI-generated content and online peer abuse?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: Process for LGB minimum testing of online safety mechanisms (termly)

Emmaus filtering systems should block harmful and inappropriate content, without unreasonably impacting teaching and learning. Tests should be carried out and recorded termly using the pro-forma overleaf to ensure that the filtering systems are working effectively.

Minimum termly testing should include:

1. **Online filtering test carried out via:** [Test Your Internet Filter | SWGfL Test Filtering]

Process to follow:

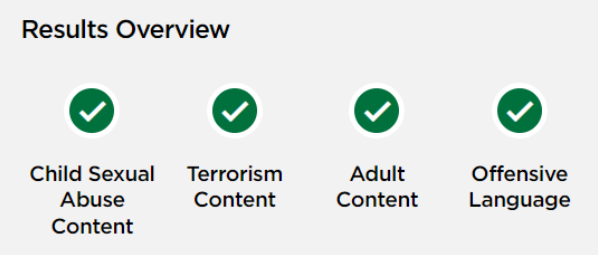
- Select Schools
- Input individual school name and postcode
- Select Smoothwall as the Filtering Provider
- Press Run Filtering Test

What to look for?

The Results Overview should show 4 green ticks for the different areas of filtering:

- Child Sexual Abuse Content
- Terrorism Content
- Adult Content
- Offensive Language

If the area shows a green tick, this indicates that the content is being blocked effectively.



There is a Description and Results & Recommendations section displayed for each of these areas of Filtering which can inform if there are any actions that need be taken.

There is also a Filter Test History which can identify any trends.

2. **Phrase test**

A phrase test is used to check that harmful and inappropriate content is being blocked when users search certain key words or phrases. This test should be completed on a number of different devices, such as in different geographical areas across the site and on different user groups e.g. staff, pupil, guests.

Each time this test is completed, different key words and phrases must be used and should be recorded. General key words and phrases should be searched along with contextualised words and phrases.

Examples may include: explosives, casinos, gambling, alcohol, pornography etc.

LGB MINIMUM TESTING OF ONLINE SAFETY MECHANISMS			
School Name			
Term		**Date**	
LGB Representative Name		**DSL/DDSL Name**	
Online Filtering Check Completed (tick)			

Section	**Green ticks to indicate content blocked**	**Action Required (Y/N)**	**Action Taken (Y/N)**
Child Sexual Abuse Content			
Terrorism Content			
Adult Content			
Offensive Language			

If any of the areas above do not show a green tick, indicating that the content is NOT blocked, then the Action Required box must be completed and this form must be forwarded to the Strategic ICT Lead immediately. If action is required, Strategic ICT Lead should complete the box below to indicate what action has been taken.

Action taken by ICT team (If applicable)	**Date**
	Signed

Phrase Test Completed (tick)	

Device tested (delete as appropriate)	**Geographical location of device (e.g. D Block, main office)**	**Type of device (e.g. iPad, laptop)**
Pupil/Staff/Guest		

Key Words or Phrases Used	**Content Blocked (Y/N)**	**Action Required (Y/N)**	**Action Taken (Y/N)**

If any of the key words or phrases are not blocked, allowing access to harmful or inappropriate content, the Action Required box must be completed and this form must be forwarded to the Strategic ICT Lead immediately. If action is required, Strategic ICT Lead should complete the box below to indicate what action has been taken.

Action taken by ICT team (If applicable)	**Date**
	Signed

Signed (LGB Representative)	
Signed (DSL/DDSL)	