EMMAUS
CATHOLIC MAC

Online Safety Policy

Version	3.0
Date created/updated	14th September 2023
Ratified by	Compliance Committee
Date ratified	17th September 2023
Date issued	September 2023
Policy review date	August 2024
Post holder responsible	Strategic ICT Lead

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 17th September 2023 and will be reviewed in August 2024.

Signed by Director of Emmaus Catholic MAC: J Griffin

Signed by CSEL for Central Team: S Horan

Schools to which this policy relates:

Signed by Principal for – Hagley Catholic High School
Signed by Principal for – Our Lady of Fatima Catholic Primary School:
Signed by Principal for – Our Lady & St Hubert's Catholic Primary School:
Signed by Principal for – St Ambrose Catholic Primary School:
Signed by Principal for – St Francis Xavier Catholic Primary School:
Signed by Principal for – St Gregory's Catholic Primary School:
Signed by Principal for – St Joseph's Catholic Primary School
Signed by Principal for – St Mary's Catholic Primary School:
Signed by Principal for – St Philip's Catholic Primary School:
Signed by Principal for – St Wulstan's Catholic Primary School:

Contents

DEFINITIONS

The Company's standard set of definitions is contained at Definition of Terms – please refer to this for the latest definitions.

1.0 Aims

1.1 Emmaus Catholic Multi Academy Company ("the MAC") aims to have robust processes in place to ensure the online safety of pupils, staff, directors, governors and volunteers and to identify and support groups of pupils that are potentially at greater risk of harm online than others.

1.2 We aim to deliver an effective approach to online safety, which empowers us to protect and educate the whole MAC community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones'). The MAC will establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

1.3 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.

2.0 Legislation and Guidance

2.1 This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, **Keeping Children Safe in Education (Sept 2023),** and its advice for schools on:

(a) Teaching online safety in schools.
(b) Preventing and tackling bullying and cyber-bullying: advice for Principals and school staff.
(c) Relationships and sex education.
(d) Searching, screening and confiscation.

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

2.3 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.

2.4 The policy also takes into account the National Curriculum computing programmes of study.

2.5 This policy complies with our funding agreement and articles of association.

3.0 Roles and Responsibilities

3.1 The Local Governing Body ("the LGB")

3.1.1 The LGB has overall responsibility for monitoring this policy and holding the (Executive) Principal to account for its implementation in School.

3.1.2 The LGB will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

3.1.3 The LGB will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

3.1.4 The LGB will co-ordinate termly meetings with appropriate staff to both discuss and test the online safety mechanisms in place. The Safeguarding Governor and the Designated Safeguarding Lead (DSL) will actively run filter and search term tests termly, documenting accordingly and liaising as necessary with the Strategic ICT Lead. Online safety logs as provided by the DSL should be monitored and reviewed appropriately (please see Appendix 5). The LGB should ensure children are taught how to keep themselves and others safe, including keeping safe online.

3.1.5 The LGB must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness (please see Appendix 5). The Directors will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually (the Strategic ICT Lead will meet with DSLs and Safeguarding Governors to do this);
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;

- Having effective monitoring strategies in place that meet their safeguarding needs.

3.1.6 All LGB Members will:

- Ensure that they have read and understood this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3).
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with 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 CSEL/(Executive) Principal

3.2.1 The (Executive) Principal is responsible for ensuring that school staff understand this policy, and that it is being implemented consistently throughout the school.

3.2.2 The (Executive) Principal must report any online safety issues or incidents to the LGB and Catholic Senior Executive Leader (CEO).

3.2.3 The Catholic Senior Executive Leader (CEO) is responsible for ensuring that Central Team staff understand this policy, and that it is being implemented consistently throughout the MAC.

3.3 The Designated Safeguarding Lead (the "DSL")

3.3.1 Details of the school's Designated Safeguarding Lead (DSL) [and Deputy/Deputies] are set out in each school's Child Protection and Safeguarding policy.

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

- Supporting the (Executive) Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the (Executive) Principal and Local Governing Body to ensure the implementation of this policy.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks: The DSL will receive a notification via email from Smoothwall of any transgression by a pupil.

- Working with the Strategic ICT Lead to make sure the appropriate systems and processes are in place.
- Working with the (Executive) Principal, Strategic ICT Lead 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's child protection policy.
- Ensuring that any online safety incidents are logged on the school's Safeguard system 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 half-termly reports on online safety in school to the (Executive) Principal which will be shared with the Local Governing Body as part of the (Executive) Principal's report to the LGB.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

  This list is not intended to be exhaustive.

3.4 The Strategic ICT Lead

3.4.1 The Strategic ICT Lead is responsible for:

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

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

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

3.5.1 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 MAC/school's ICT systems and the internet (Appendix 3), and ensuring that pupils follow the MAC/school's terms of acceptable use (Appendices 1 and 2).
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by alerting the Strategic ICT Lead.
- Following the correct procedures by contacting the Emmaus MAC ICT Support Team if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged via the school's Safeguard system 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/Carers

3.6.1 Parents/carers are expected to:

- Notify a member of staff or the (Executive) Principal of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the MAC/school's ICT systems and internet (Appendices 1 and 2).
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre

- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

3.7.1 Visitors and members of the community who use the MAC/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).

4.0 Educating Pupils about Online Safety

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

4.2 All schools have to teach:

- Relationships education and health education in primary schools.
- Relationships and sex education and health education in secondary schools.

4.3 Applicable to Emmaus Catholic Multi Academy Company Primary Schools

4.3.1 In **Key Stage 1**, pupils will be taught to:

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

4.3.2 Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

4.3.3. **By the end of primary school, Emmaus pupils will know:**

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.

- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

4.4 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.

4.5 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.

4.6 By the end of secondary school, Emmaus 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 that carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5.0 Educating Parents about Online Safety

5.1 The school will raise parents/carers' awareness of internet safety via a range of methods such as letters or other communications home, parents' evenings or in information via our website. This policy will also be shared with parents/carers.

5.2 The school will let parents/carers know:

- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

5.3 If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the (Executive) Principal and/or the DSL.

5.4 Concerns or queries about this policy can be raised with any member of staff or the (Executive) Principal.

6.0 Cyber-bullying

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

6.2 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.

6.3 Each MAC 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. Class teachers/form teachers will discuss cyber-bullying with their tutor groups.

6.4 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.

6.5 All staff, directors, 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).

6.6 Each MAC school will send 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.

6.7 In relation to a specific incident of cyber-bullying, each MAC school will follow the processes set out in the relevant 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.

6.8 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.

6.9 Examining Electronic Devices

6.9.1 Emmaus MAC staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for, confiscate and, in exceptional circumstances delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they have reasonable grounds for suspecting:

- It poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

6.9.2 Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the (Executive) Principal / DSL / appropriate staff member.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.

- Seek the pupil's co-operation.

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

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

6.9.4 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).

6.9.5 When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material constitutes evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves.

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

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

6.9.7 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

- Each school's Behaviour Policy / searches and confiscation policy.

6.9.8 Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the Emmaus Catholic MAC Complaints Procedure.

7.0 Acceptable use of the Internet within Emmaus Catholic MAC

7.1 All pupils, parents/carers, staff, volunteers, directors and governors are expected to sign an agreement regarding the acceptable use of the MAC/school's ICT systems and the internet (Appendices 1 to 3). Visitors will be expected to read and agree to the MAC/school's terms on acceptable use if relevant.

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

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

7.4 More information is set out in the acceptable use agreements in Appendices 1,2 and 3.

8.0 Pupils Using Mobile Devices in School

8.1 Reference should be made to the individual school policy on mobile devices in school.

8.2 Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see Appendices 1 and 2).

8.3 Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the individual school's Behaviour Policy, which may result in the confiscation of their device.

9.0 Staff using Work Devices Outside Emmaus Catholic MAC

9.1 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 with strong passwords.
- Making sure the device locks if left inactive for a period of time.

- Not sharing the device among family or friends.
- Keeping operating systems up to date and installing the latest updates.

9.2 Staff members must not use the device in any way which would violate the MAC/School's terms of acceptable use, as set out in Appendix 3.

9.3 Work devices must be used solely for work activities.

9.4 If staff have any concerns over the security of their device, they must seek advice from the Emmaus Catholic MAC ICT Support Team.

10.0 How the MAC/School will Respond to Issues of Misuse

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

10.2 Where a staff member misuses the MAC/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 Emmaus Catholic MAC Disciplinary Policy & Procedure and Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

10.3 The MAC/School's will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11.0 Training

11.1 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.

11.2 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, ebulletins and staff meetings).

11.3 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

11.4 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.

11.5 The DSL (and deputy/deputies) will undertake annual (refresher if applicable) child protection and safeguarding training, which will include online safety.

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

11.7 Volunteers will receive appropriate training and updates, if applicable.

11.8 More information about safeguarding training is set out in each school's Safeguarding Policy (including Child Protection).

12.0 Monitoring Arrangements

12.1 The DSL logs behaviour and safeguarding issues related to online safety via the school's Safeguard system and in line with this policy.

12.2 This policy will be reviewed every year by the Strategic ICT Lead. At every review, the policy will be shared with the Directors, Local Governing Bodies, Principals and school staff. The review will be supported by the LGfL Annual Online Safety Audit & 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.

12.3 This policy will be reviewed every year by the Strategic ICT Lead. At every review, the policy will be shared with the Directors, Local Governing Bodies, Principals and school staff. The review will be supported by the LGfL Annual Online Safety Audit & 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.

13.0 Links with other Policies

13.1 This Online Safety Policy is linked to our:

- School Safeguarding Policy (including Child Protection)
- School Behaviour Policies
- Emmaus Catholic MAC Disciplinary Policy & Procedure
- Data protection policy and privacy notices
- Emmaus Catholic MAC Complaints Policy & Procedure
- Keeping Children Safe in Education (Sept 2023)

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
• Use MAC/school computers for school work only
• Be kind to others and not upset or be rude to them
• 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
• 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 • 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.**	
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 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?	
Are you familiar with the filtering and monitoring systems on the MAC/school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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:

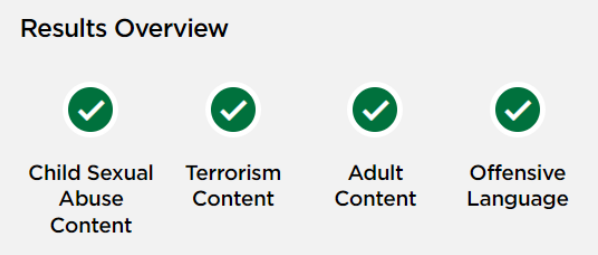
- Select Schools
- Input individual school name and postcode
- Select Smoothwall as the Filtering Provider
- Press Run Filtering Test

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)	