Online Safety Policy and Acceptable Use Agreements

ST CLARE
Catholic Multi Academy Trust

Emmaus Catholic and Church of England Primary School

Approved by:	LAC	**Date:**	March 2026
Last reviewed on:	Spring 2026		
Next review due by:	Spring 2027		

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

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

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study. This policy complies with our funding agreement and articles of association. This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, work placement students, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

3. Roles and responsibilities

Online safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

3.1 The Local Academy Committee

The Local Academy Committee (LAC) has overall responsibility for monitoring the effectiveness of implementation of this policy in their school by holding the headteacher to account for its implementation. In carrying out this duty the LAC will seek assurance that:

- All staff undergo online safety training as part of child protection and safeguarding training and 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.

- All staff understand their expectations, roles and responsibilities around filtering and monitoring.

- Pupils at the school are the taught how to keep themselves and others safe, including online. Teaching should be appropriately adapted for children with SEND, or where children have other specific needs, experiences or vulnerability, recognising that a 'one size fits all' approach may not be appropriate for all children in all situations.

- The school has appropriate filtering and monitoring systems in place on school devices and school networks, and that there is appropriate regular review of effectiveness with the IT service provider. The LAC will seek evidence that:

    - Clear roles and responsibilities have been assigned to manage filtering and monitoring systems

    - Filtering and monitoring provisions are reviewed at least annually

    - There is effective blocking of harmful and inappropriate content without unreasonably impacting teaching and learning

To carry out this duty, the LAC will ensure that the nominated safeguarding link governor meets with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL). The LAC will also ensure that they receive assurance through termly reports and evidence of monitoring and audit of online safety.

3.1 The Local Academy Committee

All members of the LAC will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3)
- Make sure that online safety is considered as an integral theme when devising and implementing whole-school safeguarding policies, procedures and practice

The governor who oversees online safety is **Gemma Murray**.

The role of the Online Safety Governor includes:

- Regular meetings with the Online Safety Lead
- Regular monitoring of Online Safety incident logs
- Reporting to Local Academy Committee

3.2 The headteacher and online safety lead

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

- The Headteacher has overall responsibility for online safety of all members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The headteacher and senior leadership team are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues when necessary.

- The headteacher and senior leadership team will ensure that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- The senior leadership team will receive monitoring reports from the Online Safety Lead.
- The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious online safety incident.
- The headteacher and senior leadership team should receive update reports from the incident management team

3.3 The designated safeguarding lead (DSL) and designated safeguarding deputies

Details of the school's designated safeguarding lead (DSL) and deputies are available within school and on our website. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- 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 ICT manager (Phil Woodcock IT Lead, St Clare's CMAT, Wave9 Filtering and Monitoring, Wavenet ICT Support)

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on 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 school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- The school receives a full safeguarding report on the filtering and monitoring of the school's ICT systems on a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Reading, understanding and helping promote the school's online safety policies and guidance.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Reporting any suspected misuse or problem to the online safety coordinator.
- Developing and maintaining an awareness of current online safety issues and guidance.
- Modelling safe and responsible behaviours in their own use of technology.
- Ensuring that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
- Embedding online safety messages in learning activities across all areas of the curriculum.
- Supervising and guiding pupils carefully when engaged in learning activities involving technology.
- Ensuring that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- Being aware of online safety issues related to the use of mobile phones, cameras and wearable devices.
- Understanding and being aware of incident-reporting mechanisms that exist within the school.
- Maintaining a professional level of conduct in personal use of technology at all times.
- Ensuring that sensitive and personal data is kept secure at all times by using encrypted data storage and by transferring data through secure communication systems.
- 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 reporting it to the headteacher or online safety lead and IT provider, contacting parents where necessary.
- Following the correct procedures by contacting Wavenet or Wave9 if they need to bypass the filtering and monitoring systems for educational purposes. Also ensuring that any bypassing of the filtering and monitoring system for educational purposes is time-bound.

- Working with the online safety lead to ensure that any online safety incidents are logged through CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Support the school in promoting online safety
- Be responsible for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss online safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly
- Model safe and responsible behaviours in their own use of technology
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Refrain from using mobile phones on site at the start and finish of the school day and to limit their use of mobile phones on site at the request of school staff.

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
- Parent resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3). All visitors are to refrain from using their mobile phones onsite at the request of the headteacher, except where express permission has been given otherwise.

4. Educating pupils about online safety

Pupils will be taught about online safety as an integral part of the curriculum, including within computing, PSHE and other lessons. Online safety is also promoted through a planned programme of assemblies and whole-school activities, including Safer Internet Day.

We will discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.

We will remind pupils about their responsibilities through an Acceptable Use Policy (Appendices 1 and 2) which every pupil will sign/will be displayed throughout the school/will be displayed when a pupil logs on to the school network.

In **Key Stage (KS) 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

Pupils in **Key Stage (KS) 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

By the **end of primary school**, 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

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.

4.1 Pupils will be taught practical cyber security skills

The DfE's non-statutory cyber security standards for schools and colleges sets out content that pupils should be taught.

All pupils should receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information

- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils should also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

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

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the online safety or class teacher.

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

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

We encourage pupils not to suffer in silence. We promote the use of strategies to enable cyber-bullying to be uncovered including:

- Philosophy for Children sessions (P4C)
- PSHE sessions
- Computing sessions
- Pastoral support

How we address cyber-bullying is covered as part of our behaviour and anti-bullying policies.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

A member of the safeguarding team will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

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

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

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

- Assess 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 a member of the safeguarding team
- 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

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

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

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

If inappropriate material is found on the device, it is up to a member of the safeguarding team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

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

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

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

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

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

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

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

7.Managing online risks

7.1 Data Protection and GDPR: Passwords

Data Protection and GDPR is covered separately in our GDPR Policy. Staff and children sign an Acceptable Use Policy (see section 8 and Appendices 1-3), which sets out appropriate behaviour, including how to protect access to usernames and passwords.

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Pupils at Key Stage 1 and above will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school. For using the iPads, children are designated a numbered iPad, which allows staff to identify who uses which device.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All information systems require end users to change their password at first log on.
- Users should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.

7.2 Data Protection: Management of assets

The school is responsible for ensuring access to ICT systems are as safe and secure as reasonably possible. All access to school ICT systems is based upon a 'least privilege' approach. Servers and other key hardware and infrastructure are located securely with only appropriate staff permitted access.

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006. Further information can be found on the Environment Agency website.

7.3 Inappropriate content: filtering and monitoring

- The school uses a filtered internet service. The filtering system is provided by Wave9.
- The school's internet provision includes filtering appropriate to the age and maturity of pupils.
- The school will always be proactive regarding the nature of content that can be viewed through the school's internet provision.
- The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Online Safety Lead. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the Online Safety Lead. The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP (Education from the National Crime Agency) or the IWF (Internet Watch Foundation).
- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked. Any non-permanent bypassing of the filtering and monitoring system for educational purposes is time-bound and includes a request to re-block after a certain date.
- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.

- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

7.4 The use of digital images and videos

Staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, including on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Images and videos should be taken with the consent of the child and they have the right to withdraw their consent at any time.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

7.5 Protecting the professional identity of staff, work placement students and volunteers

Communication between adults and between children / young people and adults, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

When using digital communications, staff, students and volunteers should:

- Only have contact with children and young people for solely professional reasons and in accordance with the policies and professional guidance of the school, for example through an online homework platform or virtual learning environment such as Seesaw or TT Rock Stars.
- Not share any personal information with a child or young person e.g. should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- Not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- Be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- Ensure that all communications are transparent and open to scrutiny.
- Ensure that if they have a personal social networking profile, details are not shared with children and young people in their care (making every effort to keep personal and professional online lives separate).
- Not send or accept a friend request from any current pupils on any forms of social media (unless they are a family member and over 13). This also includes any ex-pupils who are under 18 or are still attending secondary education. Adults in school should exercise extreme caution in accepting any ex-pupils over 18, unless there is a pre-existing personal relationship.
- Not post information online that could bring the school into disrepute.
- Ensure that all communications are transparent and open to scrutiny.
- Be careful in their communications with children so as to avoid any possible misinterpretation.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

7.6 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

8. Acceptable use of the internet in school

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

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

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

The following paragraph will also be shared with staff, volunteers and governors to provide additional guidance.

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will **not**:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way that could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

More information is set out in the acceptable use agreements in appendices 1 to 3.

9. Pupils using mobile devices in school

Pupils in upper KS2 may bring mobile devices into school. These are handed into a member of staff at the beginning of the day, kept securely through the school day and then handed back to the pupil as they leave school. No wearable tech (e.g. smart-watches or smart-rings) is permitted.

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

10. Staff using work devices outside school

All staff members must take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

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

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Staff may need to use their personal devices outside of school for work purposes. This may include using their mobile phones to make or receive phone calls from school on a trip or referring to a work email on a personal device.

When this takes place, staff should ensure they are taking appropriate steps to ensure their devices remain secure (e.g. ensuring their device has security measures in place, the use of a secure browser). If any documents are automatically downloaded onto a personal device that contains personal information (e.g. an incident report from our online information sharing system), these documents should be immediately deleted from the device after reading. Staff should consider whether they need to download that document at that time or whether it should wait until they can read it on a work device.

Staff should be mindful of sharing personal information over a telephone call within the earshot of children and members of the general public

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from ICT Manager (see 3.4).

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy, anti-bullying, data protection and acceptable use policies, as appropriate. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will report incidents that involve illegal activity or content, or otherwise serious incidents, to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The safeguarding team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety through CPOMS, our online monitoring system

This policy will be reviewed every year by the Online Safety Lead. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy and anti-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- St Clare's CMAT acceptable use policy
- St Clare's CMAT social media policy

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

Emmaus Catholic and C of E

Primary School

EYFS, Year 1 and 2

Pupil ICT Acceptable Use Policy 2026

This is how we stay safe when we use computers:

I will ask an adult if I want to use the computer.

An adult will watch me using the ICT equipment.

I will only use activities that an adult has told or allowed me to use.

I will take care of the computer and other equipment.

I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.

I will tell an adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……

Signed (parent): ……..

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

Emmaus Catholic and C of E Primary School KS2 Pupil ICT Acceptable Use Policy 2026

For my own safety:

- I understand that the school will watch my use of ICT, email and other digital communications. An adult will be supervising my use at all times.
- I will not share my username and password with anyone or try to use any other person's username and password.
- I will be aware of "stranger danger", when I am on-line.
- I will not share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any upsetting or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I understand that school ICT is for teaching and learning and I will not use it for personal use unless I have permission to do so.
- I will not use the school ICT systems for on-line gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- I will respect other people's work and property and will not access, copy, remove or otherwise alter anyone else's files, without the owner's permission.
- I will be polite and responsible when I communicate with others.
- I will not take images of anyone without their permission.

I understand that the school has a responsibility to keep ICT secure and safe:

- I will only use my mobile phone in school if I have permission. I understand that, if I do have my own devices in school, I will follow the rules and hand it in to my class teacher or to the school office.
- I will immediately report any damage or faults involving equipment, however it may have happened.
- I will not open any attachments to emails, unless I know and trust the sender of the email.
- Social Networking sites are not allowed to be used in school, unless for educational purposes as directed by teaching staff (e.g. using YouTube for a virtual author event, interacting with my peers on TT Rock Stars).

When using the internet for research for my school work, I understand that:

- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I find is accurate, as I understand that the work of others may not be correct.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school could act against me if I am involved in incidents or inappropriate behaviour that are included in this agreement, when I am out of school as well as in school. Examples of this is cyberbullying, sending/receiving inappropriate images and misuse of personal information.
- I understand that I must follow these rules. If I don't this could mean loss of access to the school network / internet, contact with parents/carers and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have understood and agree to the rules included in the Acceptable Use Agreement.

I understand the rules and I agree to follow these rules when:

- I use school ICT and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile phones, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school e.g. through social networks, mobile phones, accessing school email, Learning Platform, website etc.

Name of Student / Pupil			
Group / Class			
Signed		Date	

Appendix 3: Acceptable Use Agreement for Staff, Governors, Volunteers and Visitors

St Clare Catholic Multi Academy Trust Acceptable Use Agreement for Staff and Volunteers

This Acceptable Use Policy is intended to ensure that school IT and communication systems are used in a safe way and are kept operational for the benefit of all in the school community.

This agreement applies any time you use any systems provided by the school, whether on school premises or remotely and from any device, school owned or personal.

School IT systems are designed to support teaching and learning, systems should primarily be used for study, teaching, or administrative purposes. The school allows for modest personal use of school systems providing the terms of this policy are not breached and that personal use is not detrimental to your duties.

Acceptable Use Policy Agreement

School systems in general:

- At all times your use of school IT systems will be consistent with the values and ethos of the school.
- A professional standard of communication is expected at all times both online and off line.
- Use of school systems must be consistent with all other school policies including those on Data Protection, Social Media and the Dignity and Mutual Respect Policy. You must read and understand these.
- Do not disclose your username or password to anyone else, or try to use any other person's username and password. If someone else knows your password change it immediately and notify IT Support staff.
- You must not use the school systems to conduct any form of commercial activity without the express permission of the Headteacher.
- You may not use any form of virtual private network or file sharing software unless authorised to do so.
- You may not install any software or attempt to run any software from any other source without the express approval of IT Support staff.

Monitoring:

- School systems are monitored and filtered for the safety of all users. You must not attempt to circumvent any monitoring and your usage can be reviewed at any time.

Communication:

- Some email can contain malicious links or code, please be vigilant for suspicious email and if you unsure check with IT Support staff before opening any email or link that you are suspicious of.
- School provided e-mail accounts may be accessed by other members of staff as deemed appropriate to ensure smooth running of the school. Access is at the discretion of a member of SMT or the IT Support staff, for example for the purposes of business continuity where a member of staff is absent through illness.
- You must only communicate with students and parents and carers using official school systems.

Using your own device:

- You may only connect your personal device (smartphone / tablet / laptop etc.) to the designated wireless network of the school and only when suitable credentials are provided by the school. You must not connect any device directly to the physical network cabling of the school. Any use of any school systems (even via your own device) is filtered and monitored.

- You must not store any personal data relating to the school, its staff or pupils, including images on personal devices, even if only temporarily. The only exception to this is that you may synchronise school mail to a personal mobile device providing that device is solely used by you and is protected by either a fingerprint or other method of locking. You must not synchronise mail to a shared device of any sort, e.g. family computer or shared tablet.
- You must not sync School Onedrive / Google Drives to personal devices.
- You may only use any password manager feature (e.g. password manager software or the password manager feature of some web browsers) to store school passwords if the device you are using is personal to you (not shared by any other family member) and is protected by a locking password or other security feature such as a fingerprint.

Data Protection:

- You must only transport, hold, disclose or share personal information about yourself or others, as outlined in the school's Data Protection Policy (or other relevant policy). You must not transfer data from school systems without the express permission of the school Data Protection Officer, unless it is covered by policy documentation. All transfers of personal data must be encrypted to prevent inadvertent data loss.
- The school data protection policy requires that any staff or student data to which you have access, will be kept private and confidential, except when it is deemed necessary that you are required by law or by school policy to disclose such information to an appropriate authority.
- If you become aware of a data breach, potential or actual, you have a duty to report it to the data protection officer as soon as you become aware of the breach.

Acceptable Use Policy Agreement

I have read and understand the School Workforce (Staff and Volunteer) Acceptable Use Policy and I agree to use school systems according to this policy.
I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to action under the school's disciplinary policy, and in the event of illegal activities, the involvement of the police.

Name:	
Signed:	
Date:	

Appendix 4: Permissions for Communications Technologies

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on mobile phones or other camera devices	x No mobiles						x	
Use of handheld devices eg PDAs, PSPs	x							x
Use of personal email addresses in school, or on school network		x						x
Use of school email for personal emails		x						x
Use of chat rooms / facilities in lessons (e.g. use of YouTube Live for a virtual author visit)		x					x	
Use of instant messaging in lessons				x				x
Use of social networking sites in lessons for educational purposes (e.g. use of ClassDojo or Facebook to communicate with parents)	x						x	
Use of social networking in lessons for non-educational purposes				x				x
Use of blogs in lessons		x					x	
Wearable tech (where notifications are switched off when with pupils)	x							x