St Matthew's CE Primary School

Online Safety Policy

ST MATTHEW'S
CE PRIMARY SCHOOL

Created by:	E Tyrer	**Date:** February 2023
Approved by:	Full Governing Body (via GHub)	**Date:**
Last reviewed in:	January 2026	
Next review due by:	January 2027 Policy to be reviewed annually, or sooner if significant changes occur in technology or legislation	

ST MATTHEW'S
CE PRIMARY SCHOOL

Introduction

As a UNICEF Gold Rights Respecting School, St Matthew's CE Primary School places the UN Convention on the Rights of the Child at the heart of our ethos and culture, fostering well-being and enabling every child to reach their full potential. Our school is a place where children's rights are learned, taught, practised, respected, protected, and promoted. This commitment to children's rights and equal opportunities underpins our inclusive approach.

Article 17 of the UN Convention on the Rights of the Child states:

Children 'have the right to get information that is important to your wellbeing, from radio, newspaper, books, computers and other sources. Adults should make sure that the information you are getting is not harmful, and help you find and understand the information [they] need.'

This policy ensures that the school upholds Article 17 by providing safe and appropriate access to online information and resources, empowering children to navigate the digital world responsibly.

Aims

Our school aims to:

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

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk, as outlined by the UK Safer Internet Centre:

- **Content:** Exposure to illegal, inappropriate, or harmful content (e.g., pornography, fake news, hate speech, radicalisation, extremism, self-harm, suicide).
- **Contact:** Harmful online interactions with others (e.g., peer-to-peer pressure, grooming, exploitation by adults, commercial advertising).
- **Conduct:** Personal online behaviours that may lead to harm (e.g., cyberbullying, sharing inappropriate images, online harassment, privacy violations).
- **Commerce:** Risks associated with online transactions and commercial activities (e.g., online gambling, phishing, scams, inappropriate advertising).

ST MATTHEW'S
CE PRIMARY SCHOOL

Use of the Internet

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. The Internet is a part of everyday life for education, business and social interaction. Internet use is part of the statutory curriculum and a necessary tool for learning. Not only that, but the school has a duty to provide pupils with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

- access to world-wide educational resources including museums and art galleries
- educational and cultural exchanges between pupils world-wide
- vocational, social and leisure use in libraries, clubs and at home
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across networks of schools, support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- access to learning wherever and whenever convenient

How can the Internet enhance learning?

Pupils will be taught about acceptable and unacceptable internet use, with clear objectives set for each online activity. Staff will guide pupils towards online resources that align with planned learning outcomes, considering their age and maturity. Pupils will develop critical digital literacy skills, including effective online research, information location, retrieval, and evaluation.

Legislation and guidance

This policy is underpinned by statutory guidance, including the Department for Education's (DfE) Keeping Children Safe in Education 2025, and its advice for schools,

It also reflects relevant legislation, including the Education Act 1996 (as amended), the Education and Inspections Act 2006, and the Equality Act 2010. Furthermore, it aligns with the Education Act 2011, which empowers teachers with the authority to search for and delete inappropriate images or files on pupils' electronic devices when a 'good reason' exists, thereby strengthening measures against cyber-bullying. The policy also incorporates the National Curriculum's computing programmes of study.

This policy also makes reference to the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education 2025 , 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.

Roles and Responsibilities

The governing board

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

- The governing board will ensure that regular meetings are held with appropriate staff to discuss online safety. They will monitor online safety logs (e.g., CPOMS) provided by the Designated Safeguarding Lead (DSL) to understand trends and the effectiveness of interventions.

All governors will:

- Ensure that 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).
- 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 special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.Suggested Improvement:

The headteacher

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

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) [and deputy/deputies] are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The Designated Safeguarding Lead (DSL) holds lead responsibility for online safety in school, including:

- Supporting the Headteacher in ensuring all staff understand and consistently implement this policy.
- Collaborating with the Headteacher, ICT Manager, and other relevant staff to address online safety issues and incidents.
- Managing all online safety incidents in accordance with the school's child protection policy.
- Ensuring all online safety incidents are logged (see Appendix 5) and managed appropriately according to this policy.
- Ensuring all incidents of cyberbullying are logged and addressed in line with the school's behaviour policy.
- Developing and delivering staff training on online safety, including facilitating the use of the self-audit tool (Appendix 4).
- Liaising with external agencies and services as required.
- Providing regular reports on online safety to the Headteacher and Governing Board.

This list is not intended to be exhaustive.

The ICT Technician

The ICT technician is responsible for:

- Implementing and maintaining appropriate security protection measures, including filtering and monitoring systems. These systems will be regularly reviewed and updated to assess their effectiveness in keeping pupils safe from harmful and inappropriate online content and contact, including terrorist and extremist material.
- Ensuring the school's ICT systems are secure, protected against viruses and malware, and that all safety mechanisms are regularly updated.
- Conducting a comprehensive security check and monitoring of the school's ICT systems on a fortnightly basis.
- Blocking access to potentially dangerous websites and preventing the download of potentially harmful files.

This list is not intended to be exhaustive.

The computing curriculum leader

The computing curriculum is responsible for:

- Championing the embedding of online safety education across the curriculum.
- Supporting teaching staff by:
    - Highlighting the strong links between online safety and subjects such as RSHE, Computing, and PSHE.
    - Identifying and promoting opportunities to integrate online safety themes throughout the curriculum and school activities.
    - Guiding staff on effective monitoring of pupil online activity and risk assessment.
    - Ensuring appropriate supervision and guidance for pupils during online learning activities.
- Overseeing the logging and appropriate management of online safety incidents (see Appendix 5) in line with this policy.
- Ensuring cyberbullying incidents are addressed in accordance with the school's behaviour policy.
- Leading the annual organisation of Safer Internet Day.
- Providing strategic leadership and direction for online safety.
- Ensuring comprehensive and up-to-date online safety resources are available.
- Promoting and modelling positive online safety behaviours.

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers will:

Maintain a thorough understanding of this policy.

- Consistently implement this policy.
- Agree to and adhere to the terms of the acceptable use of the school's ICT systems and the internet (Appendix 3), and ensure pupils adhere to the school's acceptable use agreements (Appendices 1 and 2).
- Collaborate with the DSL to ensure that all online safety incidents are logged (see Appendix 5) and managed appropriately in line with this policy.
- Ensure that all incidents of cyberbullying are addressed appropriately in line with the school's positive relationships and behaviour policy.
- Respond appropriately to all reports and concerns regarding sexual violence and/or harassment, both online and offline, fostering a proactive and vigilant

This list is not intended to be exhaustive.

Parents/carers

Parents/Carers are expected to:

- be aware of and comply with this policy for the benefit of their children
- notify a member of staff or the headteacher of any concerns or queries regarding this policy
- work in partnership with the school
- promote and model positive online safety behavior
- ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

Pupils

Pupils are expected to:

- be aware of and comply with this policy
- be expected to sign the acceptable use agreement and will be encouraged to adopt safe and responsible use of the internet
- be supported in building resilience to radicalisation by providing a safe online environment

ST MATTHEW'S
CE PRIMARY SCHOOL

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).

Educating pupils about online safety

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

All schools have to teach:

Relationships education and health education in primary schools

Relationships and sex education and health education in secondary schools

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

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

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.

Educating parents/carers about online safety

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

Online safety will also be covered during parents' workshops and/or parents' evenings.

The school will let parents know:

- what type of activities their children are being asked to complete online
- if parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Deputy Headteacher and/or the DSL.

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

Dealing with safety issues

How will e-safety complaints be handled?

Parents and pupils will need to work in partnership with staff to resolve issues where these arise, and when it is appropriate to do so. Any complaint about staff misuse must be referred to the headteacher. All online safety complaints and incidents will be recorded by the school on CPOMS — including any actions taken.

Cyber-bullying

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 positive relationships and behaviour policy / anti-bullying policy.)

Preventing and addressing cyber-bullying

Cyber-bullying (along with all forms of bullying) will not be tolerated in school. It will be treated and dealt with in much the same way as bullying.

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

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

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

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

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school positive relationships and behaviour policy and anti-bullying policy. Where illegal, inappropriate or harmful

material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will 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.

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 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
- is covered within authorised searches in the Positive Relationships and Behaviour Policy.

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 headteacher/DSL
- explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- seek the pupil's cooperation.

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

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

- cause harm, and/or
- undermine the safe environment of the school or disrupt teaching, and/or
- commit an offence

If inappropriate material is found on the device, it is up to the headteacher/the staff member in conjunction with the DSL 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 refuses to delete the material themselves

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

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

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

- the DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Positive Relationships and 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.

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.

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

Pupils using mobile devices in school

Pupils in Year 6, who travel to and from school independently, may bring mobile devices into school where permission is given, but are not permitted to use them during:

- The school day
- Clubs before or after school, or any other activities organized by the school

Mobile phones are locked away in a safe throughout the school day.

Parents/carers must give permission for pupils to carry a mobile phone to and from school for emergency contact. Both parents/carers and pupils must sign a Mobile Phone Use Agreement, which agrees that pupils will not use their mobile phone on the school site at any time, including before and after school.

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

Staff using work devices outside school

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

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

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

Work devices must be used solely for work activities apart from incidental personal use, as set out in our Electronic Information and Communications Policy.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

How the school will respond to issues of misuse

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

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

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

Training

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

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

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

- technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

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

The DSL and deputy DSL 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 / 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.

Monitoring arrangements

Staff will work alongside the DSL/deputy DSL to log behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the computing lead. At every review, the policy will be shared with the governing board.

Links with other policies

This online safety policy is linked to our:

- Safeguarding and child protection policy
- Positive relationships and behaviour policy
- Anti-bullying policy
- Child on Child abuse policy
- Suspension and Exclusion policy
- Relationships, Health and Sex Education policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

ST MATTHEW'S
CE PRIMARY SCHOOL

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

EYFS Acceptable Use Policy

Staying safe whilst using the computer

To help me stay safe using computers and tablets...

I will only use a computer or tablet when an adult tells me I can.

I will tell an adult if I see something on the computer that makes me unhappy.

To help me stay safe using computers and tablets...

I will only use a computer when an adult tells me I can.

I will keep my password safe and not share it with anyone.

I will always send polite messages.

I will tell an adult if I see something that makes me unhappy or unsafe.

ST MATTHEW'S
CE PRIMARY SCHOOL

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

KS2 Acceptable Use Policy

Staying safe whilst using computers and tablets

To help me stay safe using computers and tablets...

I will ask permission before using the Internet and use it for a specific purpose.

I will never share my personal details, such as my full name or address, with people I don't know.

I will never share my password with anyone.

I will never meet up with someone I have met on the Internet.

I will always check my messages are polite before I send them.

I will not reply to a message that isn't kind, but I will save it and show it to an adult.

I will not open or download a file unless I am sure it is safe or I have checked with an adult.

I know I should not believe everything I read on the Internet.

I will always tell an adult if something I see makes me or my friends unhappy or unsafe.

ST MATTHEW'S CE PRIMARY SCHOOL

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

Acceptable use of the school's ICT systems and internet: agreement for staff, governors, volunteers and visitors

Staying safe whilst using ICT and the Internet

Name of staff member/governor/volunteer/visitor:

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

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

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

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 school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
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: online safety incident report log

To be recorded on CPOMS – this can be used as a guide or backup

online safety incident log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 6: Introducing the Policy

How will the policy be introduced to pupils?

- Pupil instruction in responsible and safe use should precede Internet access.
- All users will be informed that network and Internet use will be monitored.
- A different element of e-safety will be taught to children each year in the first half-term.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum.
- Each unit of the computing curriculum will include elements of e–safety.
- Particular attention will be given where pupils are considered to be vulnerable.
- Children must sign when they have read and understood the AUP.
- The AUP will be displayed in rooms with Internet access.

How will the policy be discussed with staff?

- The online safety policy will be formally provided to and discussed with all members of staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- The staff AUP will be posted in areas most used by teaching staff.

How will parents' support be enlisted?

- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–safety at other attended events e.g. parent evenings, sports days.
- At least one parent workshop will be held every year to keep parents updated on the risks involved in using the Internet and what they can do to help prevent them.
- Advice on filtering systems and responsible use of the Internet (including social networks) will be made available to parents.
- Parents' attention will be drawn to the school online safety policy on the school website.

ST MATTHEW'S CE PRIMARY SCHOOL

Appendix 7: Implementation Guidance

How will email be managed?

Pupils may only use approved school email accounts (Google for Education Mail). As a default, these should only allow children to email other children within the school, but could be changed dependent on needs of the class as long as this was strictly monitored (allowing children to email outside of the school).

Pupils must not reveal personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission from an adult. They must immediately tell a teacher if they receive an offensive email. The forwarding of chain messages is not permitted.

Staff should only use school email accounts to communicate with colleagues or when contacting a parent or an outside organisation on behalf of the school.

Emailing will be kept within the safe boundaries of the Purple Mash programme in Early Years and KS1. Pupils in Upper KS2 may be entitled to use their Google for Education Mail accounts to approved recipients under supervision from a member of staff.

How will social networking, social media and personal publishing be managed?

The school filters access to social networking sites so these cannot be accessed by pupils using the school network. Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised to never give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs, etc.

Teachers are advised not to run social network spaces for pupil use on a personal basis. Instead, the school website should be used as an official communication channel between the school and pupils. Official school blogs or wikis should be password protected and linked to from the school website.

When using blogs, pupils should be advised on security, encouraged to set passwords and to deny access to unknown individuals, and instructed to block unwanted communications. Pupils should be encouraged to use the blogs for posting and commenting on work, rather than as a form of communication. They should be advised not to publish specific and detailed private thoughts.

How would video-conferencing be managed?

The equipment and network

All video-conferencing equipment in the classroom must be switched off when not in use, not set to auto answer and have the lens cap on. External IP addresses should not be made available to other sites. Video-conferencing contact information should not be put on the school Website. The equipment must be secure and if necessary locked away when not in use. School video-conferencing equipment should not be taken off school premises without permission.

Users

Only key administrators should be given access to the video-conferencing system, web or other remote control page available on larger systems. Unique login and password details for the educational video-conferencing services should only be issued to members of staff and kept secure. Children should not use video-conferencing equipment unless supervised by a teacher or learning assistant. The school will inform parents or carers when recording/streaming during a video conference with other schools or external

organisations, and gain parental consent. At any stage in a video-conference, users should know how to stop the call.

Content

Video-conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity. Video-conferencing should be supervised appropriately for the pupils' age. A dialogue should be established with other conference participants before taking part in a video-conference. If it is a non-school site, it is important to check that they are delivering material that is appropriate for the class. It is recommended that content is sought and booked through the JVCS content providers website: https://community.ja.net/groups/vc-content-providercatalogue

How can emerging technologies be managed?

- emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- staff should not use mobile phones to take pictures or videos of children unless this is with written permission from the Headteacher and guidance is followed (see: Bring Your Own Device Policy)
- staff should only use digital cameras or tablets which have been provided by the school
- mobile phones are not permitted for use anywhere in school around the pupils. This applies to members of staff and other visitors to the school. Mobile phones may only be used in office areas, the staffroom etc. or when children are not present. The only exception to this is staff taking a mobile phone with them on a school trip/visit outside of school, for use in emergencies only
- pupils who bring mobile phones to school are required to hand them in to a member of staff in the morning and then collect them at home time

How can we protect children from online extremism?

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the Internet in schools. We have an important role to play in equipping children to stay safe online. Internet safety is integral to the computing curriculum. Our staff should complete annual Prevent training so they aware of the risks posed by online activity of extremists and understand their duty to take action if they believe the wellbeing of any pupil is being compromised.

School Website and Published Content

How will published content be managed?

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Can pupils' images or work be published?

Images that include pupils will be selected carefully. Pupils' full names will not be used on the website, particularly in association with photographs. Parents or carers should be given the opportunity to refuse permission before images of pupils are electronically published.

Information Systems

How will information systems security be maintained?

The school's network is protected by Sophos anti-virus software. The virus protection is updated regularly. The security of the school information systems and users will be reviewed regularly. Portable media may not be used without prior consent from the headteacher, and not without a virus check.

Files held on the school's network will be regularly checked. The Computing Lead / IT Technician will review system capacity regularly.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How should personal data be protected?

Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act (1998), the Freedom of Information Act (2000) and the UK General Data Protection Regulation.

Assessing Risks

The school should audit IT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate. Methods to identify, assess and minimise risks will be reviewed regularly. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer, laptop, tablet or other device. Neither the school nor Trafford Council can accept liability for the material accessed, or any consequences resulting from Internet use.

The Internet

How will pupils learn how to evaluate Internet content?

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of online materials is a part of teaching and learning in every subject, not just computing.

How will web-filtering be managed?

The web filtering provision by Trafford Council operates at the network level so is not dependent on any particular type of device or software. This ensures that traffic from mobile devices and apps are also filtered when using the schools network connectivity.

Websites are organised into distinct categories and blocked or allowed based on that category. These categories are updated in real time so that new websites are categorised as soon as possible. If a website is uncategorised then the web filter will scan the page for "keywords" and then give it a score based on how many of these words or phrases it finds (in multiple languages). If the score exceeds a certain pre-determined threshold, then the website will be blocked. This threshold can be adjusted per policy.

Policies are assigned based on logon. A teacher will receive a less restrictive policy than that of a pupil. If no logon information is passed to the web filter, then a VERY restrictive default policy will be applied. Regardless of who logs on, websites of a more serious nature e.g. pornography, gambling, hate etc are blocked for all users throughout the borough.

Policies are assigned based on group memberships in schools, it is the responsibility of the school to ensure that the users are members of the correct groups. Adding users to incorrect groups could lead to inappropriate access for the users involved. Group membership in schools is polled by default every 48 hours so changes in group memberships can take this long to take effect but this can be requested immediately in urgent situations.

There is no restriction on the number of policies which a school can have so if a school felt that a KS1 and KS2 policy was needed or even individual class policies, these can be put in place although the allocation of pupils to these groups remains the school's responsibility.

As St Matthew's have our own pupil and staff policies independent of any others, the school is able to request modifications to these as required, as long as it is not deemed to be a safeguarding issue. As the school can request modifications to the policies and are effectively in control, this ensures that the council is not over-blocking any required access and restricting teaching and learning.

If staff or pupils discover unsuitable sites, the URL must be reported to the ICT manager so it can be added to the list of blocked websites. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

Reporting

Reports can be produced which are based on username, IP address, domain (school) or website. Example reports which can be produced are:

- all web access for a specified user/domain or IP address during a specified time
- all attempted access to a specified web address during a specified time
- all blocked access for specific users/domains/IP addresses
- top blocked sites for particular users/domains/IP addresses
- most web access in a particular domain or IP range

Keyword search reporting alerts are made to the council shortly after they occur. If these are deemed to be of a serious nature, then the school should be contacted.

Firewall

There is also an enterprise level firewall at the edge of the schools' WAN which stops any traffic from school systems attempting to reach the Internet directly unless explicitly allowed to do so. This firewall also stops any traffic trying to reach the schools WAN unless explicitly allowed to do so. The school can request firewall rules and these will be evaluated by the council's ICT security team. The security team will advise against allowing any type of access which they feel could place the school and the Trafford WAN in any danger. In some cases, they may refuse to put these rules in place.

How will Internet access be authorised?

All staff must read and sign the Acceptable Use Policy for Staff before using any school ICT resource. Parents/carers will be asked to sign a consent form for pupil access (as part of the Induction Pack).

In EYFS and Key Stage 1, access to the Internet will be by adult demonstration with occasional supervised access to specific, approved on-line materials or safe search engines.

Children in KS2 will be able to search the Internet (with filtering applied) but must be taught how to make searches more specific to reduce the chances of coming across inappropriate material. They should be taught to switch off their screen and tell and adult if they do happen to find inappropriate material.

ST MATTHEW'S
CE PRIMARY SCHOOL

How is the Internet used across the community?

The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/updates