St Matthew's C of E Primary School

Online Safety Policy

Introduction

At St Matthew's Church of England Primary School, we are committed to providing all children with equal opportunities to enable their light shine while staying safe online. We explicitly teach pupils the skills and knowledge they need to become creative, digitally literate and computational thinkers and in addition to that, we also teach them to stay safe whilst online. This policy sets out a framework within which teaching and non-teaching staff can work, and gives guidance on the teaching of online safety.

Aims

At St Matthew's, we aim to educate pupils so they are safe whilst online and 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 (the 4 Cs as referenced to in KCSIE)

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

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi nudes and/or pornography), sharing other explicit images and online bullying;
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying
- 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.

Roles and responsibilities

The Governing body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governor who oversees online safety is our chair of governors who is also the safeguarding governor.

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
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND. The 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 approach may often be more suitable

The Headteacher (also the DSL)

The headteacher is responsible for

- Ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Addressing any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on Safeguard
- 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

The ICT manager- Network IT24

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

All staff and volunteers

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

- Maintaining an understanding of this policy

- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet
- Working with the DSL to ensure that any online safety incidents are logged 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'

Parents

Parents are expected to:

- Notify the headteacher of any concerns or queries regarding this policy
- Parents can seek further guidance on the school website.

Educating pupils about online safety

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

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, for example within the schools PSHE curriculum. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating parents about online safety

At St Matthew's, we raise parents' awareness of internet safety in letters and in information via our website. Our Inspire workshops regularly have an online safety focus and we have ChildNet in school every three years who hold a session for parents

Cyber-bullying

Definition

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

Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- At St Matthew's, we actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Cyber bullying is part of our planned computing curriculum where all aspects of e-safety for primary children are delivered.
- All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of our annual safeguarding training
- At St Matthew's, we also send information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

Bullying and discriminatory behaviour

In aspiring to let everyone's light shine, we do not tolerate bullying or discriminatory behaviour at St. Matthew's. Our definition of bullying behaviour is shared and understood by all children and adults in our school community. It is displayed in every classroom:

Several times on purpose? Start telling other people.

'Bullying is deliberately and repeatedly saying or doing anything that makes others unhappy.' This includes physical, emotional, cyber bullying, prejudice based or discriminatory bullying. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police. Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

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

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

Acceptable use of the internet in school

- All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet
- 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.

Pupils using mobile devices in school

Pupils may bring mobile devices to school, but are not permitted to use them. All pupil mobile phones must be handed into the office at the beginning of the school day and must be switched off.

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.

Staff using work devices outside school

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

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

Staff members must not use the device in any way which would violate the school's terms of acceptable use

- 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 NetworkIT24, our ICT managers.

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. 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 procedure. 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 the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

All teaching staff complete Keeping Children Safe Online biannually

Monitoring arrangements

The DSL and staff can log behaviour and safeguarding issues related to online safety via Safeguard.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policies
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

St Matthew's Approach

'Be the same person privately, publicly and personally.'

While we appreciate the benefits of going online, we are also aware of the risks. At St Matthew's teaching online safety is at the heart of our computing curriculum and general safeguarding of children.

The Curriculum

Our Online Safety curriculum is taught alongside our computing curriculum, although we recognise it is part of our PSHE curriculum too. We also have specific safety moments throughout the year. Our anti-bullying week in the autumn gives us a chance to look at online bullying in greater depth and we also participate in Safer Internet Day in the spring term.

ProjectEvolve

As part of our computing curriculum, we use a comprehensive scheme of work to teach aspects of online safety explicitly throughout the year.

ProjectEvolve is an online resource which is constantly 'evolving' to ensure the online safety messages that children and young people are being taught are delivered in a way that is appropriate; meaningful; encourages reflection and generates positive outcomes. It is based on the UK Council for Internet Safety framework (UKCIS) and Education for a Connected World framework (EFACW) and it covers knowledge, skills, behaviours and attitudes across eight strands of our online lives from EYFS through to Year 6.

It is updated regularly to reflect our evolving world and the online content is separated into eight strands which are taught throughout the year:

1. **Self-Image and Identity:** Shaping online identities and how media impacts on gender and stereotypes
2. **Online Relationships:** Relationships and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.
3. **Online Reputation:** Strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles
4. **Online Bullying:** Strategies for effective reporting and intervention and how bullying and other aggressive behaviour relates to legislation
5. **Managing Online Information:** Strategies for effective searching, critical evaluation and ethical publishing
6. **Health, Well-being and Lifestyle:** The impact that technology has on health, well-being and lifestyle including understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.
7. **Privacy and Security:** Behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.
8. **Copyright and Ownership:** Protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution

We have also linked each of the ProjectEvolve strands to the 4 C's of online safety:

	Content	Contact	Conduct	Commerce
ProjectEvolve knowledge strands	• Managing Online Information • Copyright and Ownership	• Online Bullying • Health, Well-being and Lifestyle	• Online Reputation • Self-Image and Identity • Online Bullying • Health, Well-being and Lifestyle • Privacy and Security	• Privacy and Security • Copyright and Ownership

Content

Content is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

Conduct

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

Commerce

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.
Project Evolve knowledge definitions:

Rationale

ProjectEVOLVE isn't a curriculum or scheme of work; it's a set of resources, assessment and tracking tools that support the UK Council for Internet Safety and the Department for Science and Innovation Technology digital competencies framework "Education for a Connected World" The framework identifies what educators should focus on with children and young people at each stage of their school journey. It covers eight strands of their online lives from Early Years right through to 18 and beyond.

At St Matthew's, we select the strands that link to our Teach Computing curriculum and in addition to this, we select stands that:

- Are relevant to current affairs
- We have prioritised as being important due to the age of the children
- An issue has arisen which we have had to deal

Cross-curricular integration

The computing curriculum alone may not be the most appropriate subject in which to teach a very broad set of skills for the complex online world. There are several cross curricular opportunities which we also exploit such as: during PSHE lessons to support the teaching of self-image and identity or in English through discussions about misinformation or disinformation or fact and opinion.

Assessment

The Knowledge Map tool in ProjectEVOLVE has been designed to: '

- Assess knowledge across strands collectively for a group of children
- Return data that enables staff to prioritise statements according to the knowledge the group of children have across the strand
- Measure the impact of teaching and track progress for the group over time

An approach to planning

- Staff to select a strand (or two) on which to focus
- Run a knowledge map at the beginning of the unit to which each child from the group contributes
- Use the data to prioritise two or three statements
- Add to the planner, download and teach
- Measure impact by running the second knowledge map
- Review the impact on the dashboard

These outcomes are mapped and build on prior knowledge. The statements guide staff as to the areas they should be discussing with children as they develop their use of online technology. Therefore, children at St Matthew's cover each strand several times whilst on their online safety journey.