POLICY TYPE: PRESCRIBED
ACTION: FOR SCHOOL ADAPTION & ADOPTION

Southwark Diocesan
Board of Education
Multi-Academy Trust
Developing Church of England Education

Approval Body:	COO
Approval Date:	SEPTEMBER 2021
Version:	1 (SEPTEMBER 2021)
Policy Ref:	OSP01

POLICY HANDBOOK

ONLINE SAFETY POLICY

1. AIMS

1.1 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

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

2. LEGISLATION AND GUIDANCE

2.1 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: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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

2.3 It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

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

3. . Roles and responsibilities

3.1 **The governing board**

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

3.2 The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

3.3 The governor who oversees online safety is Alison Knibbs – Safeguarding Governor.

3.4 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, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.5 **The headteacher**

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

3.6 **The designated safeguarding lead**

Details of the school's DSL deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

3.7 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, ICT Lead/ E-Safety Co-ordinator 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 child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.8 The ICT Lead/E-Safety Co-ordinator

The ICT Lead/E-Safety Co-ordinator 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
- Ensuring that any online safety incidents are logged (see appendix 5) 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

This list is not intended to be exhaustive.

3.9 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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.

3.10 Parents

Parents are expected to:

- 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)

3.11 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
- Healthy relationships – Disrespect Nobody

3.12 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).

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

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

4.2 The text below is taken from the National Curriculum computing programmes of study.

4.3 It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

4.4 All schools have to teach:

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

4.5 In Key Stage 1, pupils will be taught to:

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

4.6 Pupils in Key Stage 2 will be taught to:

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

4.7 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

4.8 The safe use of social media and the internet will also be covered in other subjects where relevant.

4.9 Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. EDUCATING PARENTS ABOUT ONLINE SAFETY

5.1 The school will raise parents' awareness of internet safety in letters or other communications home, during curriculum open days, and in information via our website or via Arbor MIS. This policy will also be shared with parents on our website.

5.2 Online safety will also be covered during parents' evenings.

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

5.4 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 one 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

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

6.3 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 classes.

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

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

6.6 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.

6.7 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.

6.8 The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.9 Examining electronic devices

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.

6.10 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

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

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

6.12 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

6.13 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. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

7.1 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 (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

7.2 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.

7.3 We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

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

8. PUPILS USING MOBILE DEVICES IN SCHOOL

8.1 Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

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

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

9. STAFF USING WORK DEVICES OUTSIDE SCHOOL

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

- Keeping the device password-protected – 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

9.2 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.

9.3 Work devices must be used solely for work activities.

9.4 If staff have any concerns over the security of their device, they must seek advice from Jade Hills, Assistant Head and Digital Lead.

10. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

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

10.2 Where a staff member misuses the 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 staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. TRAINING

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

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

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

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

11.4 Training will also help staff:

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

11.5 The DSL and deputies 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.

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

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

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

12. MONITORING ARRANGEMENTS

12.1 The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

12.2 This policy will be reviewed every year by the Headteacher. 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.

1. APPENDIX 1: ACCEPTABLE USE AGREEMENT (PUPILS AND PARENTS/CARERS)

1: Short visits to the local area

We often take the children out on local visits in connection with their learning in the school. Local, in this case, means in or around Redhill.

On those occasions when visits involve any kind of cost or transport you will receive a letter with details and a permission slip as usual.

* **I give / do not give** permission for my child to take part in all such visits as outlined above.

2: Pupil Internet Access

All pupils use computing devices, including internet access, as an essential part of their learning.
The school uses an educationally filtered service and teaches e-safety to pupils in order to keep pupils safe and prevent them from accessing inappropriate material.

Think then Click

These rules help us to stay safe on the internet.

- We only use the internet with the permission of an adult.
- We click on buttons and links when we know what they do.
- We will tell an adult if we see anything we are uncomfortable with.
- We write polite and friendly messages to people that we know.
- We will never give out personal information or passwords.

Please discuss the above rules with your child to ensure that they understand their role in using computing devices safely and responsibly.

Parent / Guardian's Permission

** **I give / do not give** permission for my child to have internet access on the terms set out above.*

2. APPENDIX 3: ACCEPTABLE USE AGREEMENT (STAFF, GOVERNORS, VOLUNTEERS AND VISITORS)

St Matthew's CofE Primary School

Acceptable Use Agreement and ICT Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all adults using the School's ICT resources are aware of their professional responsibilities. All staff and visitors using School ICT resources are required to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with SLT or the Computing Subject Leader.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email and other messaging services and social networking, and that ICT use may also include personal ICT devices when used for school business or for communications relating to the School.

- I understand that to use a school ICT system for an inappropriate purpose may be a criminal offence.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will only use the school's email / internet / intranet / learning platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the SLT or MAT.

- I will comply with ICT system security and not disclose any passwords or access codes provided to me by the school or other related authorities.

- I understand that I am responsible for all activity carried out under my usernames on any school system.

- I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role.

- I will ensure that all electronic communications with stakeholders, including email and social networking, are made through monitored school systems only.

- I will as far as possible only use approved, secure electronic systems for any school business.

- I will not install any hardware or software without the permission of the SLT.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Reference sensitive data, I will ensure I have read, understood and am compliant with the School's GDPR guidelines and the MAT's GDPR policy.

- I will respect copyright and intellectual property rights in using internet-derived materials.

- I will support the school's E-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote E-safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will report any incidents of concern regarding children's safety to the Head Teacher, who is also the Designated Safeguarding Lead.

- I understand that all my use of the internet and other related technologies can be monitored and logged and such logs can be made available, on request, to the SLT or MAT.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Name (print)……

Job title / role within school: ……

Signature…… Date……

3. APPENDIX 5: ONLINE SAFETY INCIDENT REPORT LOG

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