Stella Maris School

E-Safety Policy

Updated:	**Sept. 2025**
Review Date:	**Sept 2026**

Stella Maris School is committed to Safeguarding and promoting the welfare and well-being of all members of the school. All school staff and volunteers who work in the school are expected to share this commitment and vision.

This Policy was written in consultation with the Trustees, Headteacher and the staff of Stella Maris School with due regard to our mission statement.

"At Stella Maris we endeavour to put the children at the centre of everything we do. Our mission is to educate, nurture and instil traditional values and cherish our children. We inspire them to achieve their best in every aspect of their lives."

Stella Maris School E-safety Policy

1. Aims

Stella Maris School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and Guidance

The E-safety Policy which we have adopted at Stella Maris School is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education 2024, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including 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 E-safety Policy also takes into account the National Curriculum computing programmes of study and is closely linked to the teaching of ICT in school and the awareness of children needing solid foundations for learning how to stay safe online.

3. Roles and Responsibilities

The Board of Trustees

The Board has overall responsibility for monitoring this E-safety Policy and holding the Headteacher to account for its implementation.

The Trustees of the school will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety updates, as provided by the Designated Safeguarding Leads (DSL).

All Trustees will:

- Ensure that they have read and understand this E-safety Policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

The Headteacher

The Headteacher is responsible for ensuring that staff understand this E-safety Policy, comply with the regulations and that it is being implemented consistently throughout the school. The senior teacher will assist her in this matter.

The Designated Safeguarding Lead and the Deputy

Details of the school's Designated Safeguarding Lead (DSL) and the Deputy are set out in our school Safeguarding Policy.

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

- The Headteacher is the DSL so will work closely with the Deputy DSL to share the task of ensuring that staff understand this Policy and that it is being implemented consistently throughout the school
- Working with other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) 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's Behaviour Policy
- Updating and delivering staff training on online safety (appendix 3 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 Board of Trustees

3.4 Management of ICT

The Headteacher will ensure that any technical support purchased by the school will:

- Put in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- Conduct a security check by monitoring the school's ICT systems on a monthly basis
- Block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files
- Ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this Policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy

3.5 All Staff and Volunteers

All 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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this Esafety Policy
- Ensure their child understoods the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites or alternatively speak to any member of staff on this topic.

Listed below are some useful sources of information for parents to access.

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advicecentre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet09-17.pdf

3.7 Visitors

Visitors or guest speakers 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 2).

4. Educating Pupils about Online Safety

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

The text below is taken from the National Curriculum computing Programmes of Study.

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

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

The school will use assemblies and whole school events like "Internet Safety Week" to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in letters or other communications and in information via our website.

This E-safety Policy will also be shared with parents.

Online safety will also be covered during parents' evenings and other E-safety events.

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

Concerns or queries about this E-safety 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.

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. This will be visited on numerous occasions during PSHE and ICT lessons as well as through workshops and dedicated assemblies. It will also form part of the Year 6 transition programme which the children access in preparation for moving to high school.

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.

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, the Board of Trustees and volunteers (where appropriate) receive training and updates on cyber-bullying, its impact and ways to support pupils, as part of their on-going safeguarding training which forms part of every staff meeting.

The school also informs parents on cyber-bullying as part of information evenings and parent meetings 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.

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.

Support will always be available for any children, parents or staff who find themselves in a situation of either being the recipient of cyber-bullying or be in a position of trying to contain it. The whole school community will work together to solve any issues which may arise.

6.3 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.

Our children are not allowed to bring personal electronic devices to school.

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 any device which has been taken into school against school rules, 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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on devices which have been brought into school against school rules will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and Board of Trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). 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.

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

8. Pupils using mobile devices in school

Pupils are not allowed to bring mobile devices into school, unless particular circumstances make it necessary for a child to have a phone for the purpose of maintaining contact with parents. In this extraordinary situation permission must be sought by the parents with the Headteacher. The phone will remain in the school office during the school day and will only be used by the child under supervision by a member of staff when the need arises.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Behaviour Policy, which will result in the confiscation of the mobile device.

During school trips or residential events children are not allowed to bring phones or mobile devices.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others.

They must take all reasonable steps to ensure the security of their work device when using it outside school.

Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Headteacher or the teacher in charge of Curriculum ICT who will call in technical support to assist in resolving the issue, if required.

Work devices must be used solely for work activities.

10. 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 the 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 procedures.

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.

11. 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 and be made aware of our procedures and policies surrounding E-safety.

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

The DSL and the Deputy 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.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding Policy.

12. Monitoring Arrangements

The DSL will log behaviour and safeguarding issues related to online safety.

An incident report log can be found in appendix 4.

This E-safety Policy will be reviewed regularly by the Headteacher.

At every review, the E-safety Policy will be shared with the Board of Trustees for approval.

A new filtering and monitoring package is in place as a response to the KCSIE 2023 updates. All online activity can be viewed and monitored by the DSL (Headteacher) and the Deputy DSL.

13. Links with other Policies

This E-safety Policy is linked to our:

- Safeguarding Policy
- Behaviour Policy
- Staff disciplinary procedures as set out in the Employees handbook

- Data Protection Policy and Privacy Notices
- Complaints Procedure

Appendix 1: Acceptable Use Agreement (pupils and parents/carers)

Children will sign an age appropriate form of this agreement with their parents/carers.

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share passwords with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline

I know that my teachers will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: Acceptable Use Agreement for Staff, Trustees, Visitors and Trustees who use the school's ICT systems.

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

Name of staff member/Trustee/visitor:

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

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- 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
- Share my password with others or log in to the school's network using someone else's details

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 school computers and devices are the property of the school and the school has the right to monitor internet activity if required.

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 E-safety Policy and the school's Data Protection Policy.

I will let the Designated Safeguarding Lead (DSL) or Deputy DSL 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.

When children in my care is using the school's ICT systems or the internet I will never leave them unsupervised.

Signed (staff member/Trustee/Visitor):	**Date:**

Appendix 3: Online Safety Training Needs – Self-Audit for Staff.

Online safety training needs audit	
Name of staff member:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
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, Trustees 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 cyberbullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: Online E-safety Incident Report Log

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