# St Joseph's Catholic Primary School, Epsom

## Online Safety Policy 2025
## Covering Acceptable Use of the Internet and Agreements

| | |
|---|---|
| Designated Safeguarding Lead (DSL) team | **Tim Hallett** - Lead<br>Jo Cullen, Heidi Shanks, Sophie Mundy, Rachel Wheeler |
| Online-safety leaders | Monika Szilagyi |
| Online-safety link governor | Dr. John Thomas |
| Computing link governor | Dr. John Thomas |
| EPR/RSE lead | Elaine Tobbitt/Rachel Wheeler |
| Network manager | SoftEgg |
| Date this policy was reviewed | September 2025 |
| Date of next review and by whom | November 2026 |

**Contents**

## 1. Introduction and 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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Take future steps to prepare pupils for changing and emerging technologies, such as generative AI, and to support their safe and appropriate use

## 2. 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: 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.

## 3. How we communicate

### 3.1 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 co-ordinate meetings with appropriate staff as required to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
The governors who oversee online safety is Dr. John Thomas

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).

The E-safety Committee will hold an annual meeting to review online safety policy and procedures and report back to Governors

### 3.2 The Headteacher

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

### 3.3 The Designated Safeguarding Lead

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

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 manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the governing board.

This list is not intended to be exhaustive.

### 3.4 ICT Support

We outsource our ICT support to SoftEgg. A technician visits once a fortnight. All CPD, support and advice is available each day both online or on the phone. SoftEgg is responsible for:

- Putting 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.
- 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. Reports are delivered automatically to the school, using SECURLY.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

### 3.5 All staff and volunteers

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

- 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 / 2).
- Working with the DSL to ensure that any online safety incidents are logged 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.

### 3.6 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).

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 factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

### 3.7 Visitors and members of the community
Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

## 4. 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.
- 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.

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

Sessions are run for parents on internet safety each year.

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. 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.

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. Teachers will discuss cyber-bullying with their classes.

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 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.

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.

### 6.3 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.

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.

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 pupils' electronic devices will be dealt with through the school complaints procedure.

## 7. 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 (appendices 1-4). 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, 2 and 3.

## 8. Pupils using mobile devices in school

Children **in year six only** may bring brick devices into school. Phones are left at the school office (or at one of the gates) before school starts and collected at the end of the day.

Children are not permitted to bring smart watches or smart phones to school.

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.

We fully support the Smart Phone Free Childhood Campaign with a parent lead WhatsApp community and articles regularly go in the family newsletters.

## 9. 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, as set out in appendix 3.

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 the Headteacher.

## 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 our policies on behaviour and ICT and internet acceptable use. 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.

## 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.

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.

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.

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

Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

## 12. Monitoring arrangements

The DSL log behaviour and safeguarding issues related to online safety. This is recorded in the DSL Summary Report which is viewed by governors.

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

## 13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

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

| Think before you click | | |
|---|---|---|
| **S** | **I will only use the internet with an adult** |  |
| **A** | **I will only click on icons and links when I know they are safe** |  |
| **F** | **I will only send friendly and polite messages** |  |
| **E** | **If I see something I don't like on a screen, I will always tell an adult** |  |

**Appendix 2: KS2 acceptable use agreement**

# The Internet Contract for Years 3 to 6

**I will:**

- only use the school's computers for schoolwork.
- only edit or delete my own files and not look at, or change, other people's files without their permission.
- keep my logins and passwords secret.
- only visit or search for sites that I know are suitable for school.
- only e-mail people I know, or a responsible adult has approved.
- only send information which is always polite and sensible.
- ask permission before opening an e-mail, downloading internet files or attachments from someone I do not know.

**I will not:**

- bring files into school without permission.
- load anything from the internet without permission.
- give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.

**I know that:**

- some websites and social networks have age restrictions and I should respect this.
- if I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.
- the school may check my computer files and the internet sites I visit.
- if I break this contract, I will lose the privilege of using the internet, either temporarily or permanently.

*I have read and understand these rules and agree to them.*

*Signed:* *Date:*

# St. Joseph's Catholic Primary School

Tel: 01372 727850

Headteacher:
Tim Hallett

email: info@stjosephs-epsom.surrey.sch.uk
website: www. stjosephs-epsom.surrey.sch.uk

Rosebank, West Street,
Epsom, Surrey KT18 7RT


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

As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment -Fronter
- ICT facilities and equipment at the school.

Please tick the following statements to indicate your agreement:

| | |
|---|---|
| | I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. |
| | I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me. |
| | Use of digital images, photography and video: **I understand the school has a clear policy on "The use of digital images and video" and I support this.** |
| | **I will not take and then share online, photographs of other children (or staff) at school events without permission, for example on Facebook, snapchat, Instagram and other similar programmes.** |
| | I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour. |
| | I understand the school is not liable for any damages arising from my child's use of the Internet facilities. |
| | **I understand that the school will necessarily use photographs or take film of my child to support learning activities. I know that this material does not enter the public domain.** |
| | I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns. |

| | |
|---|---|
| **Parent / Carer name** | |
| **Pupil name:** | |
| **Date** | |

**Appendix 3 (continued): St Joseph's Catholic School Acceptable Use Policy Information**

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 policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Tim Hallett.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

- 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 Headteacher or Governing Body.

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

- I understand that I am responsible for all activity carried out under my username.

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

- I will only use the approved, secure email system(s) for any school business.

- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.

- I will not install any hardware or software without the permission of the network manager, Softegg or without the permission of the Headteacher.

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

- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without the permission of the parent/carer, member of staff or Head teacher.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.

- I will respect copyright and intellectual property rights.

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

- I will report any incidents of concern regarding children's safety to the Headteacher either verbally or using CPOMs reporting.

- I will ensure that any electronic communications with pupils including email, IM and social networking are carried out in a professional capacity (e.g. when teaching email); that they are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- 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 students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

**User Signature**

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

Full Name……(printed)

Job title……

Signature…… Date……