St Joseph's Catholic Primary School
Exmouth

Walking with Jesus to be the best we can be

Plymouth CAST

Online Safety Policy

June 2025

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

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.

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

The Prevent Duty

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism. The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context. Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.
The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. For St Joseph's this is provided via Netsweeper – schools broadband – Jon Willcox is sent a report each week with any searches that are flagged and any blocked/inappropriate content.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups. The Prevent Duty means that all staff have

a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:
 Internet searches for terms related to extremism
 Visits to extremist websites Use of social media to read or post extremist material
 Grooming of individuals

Working Together to Safeguard Children (2018) defines extremism. It states "Extremism goes beyond terrorism and includes people who target the vulnerable – including the young – by seeking to sow division between communities on the basis of race, faith or denomination; justify discrimination towards women and girls; persuade others that minorities are inferior; or argue against the primacy of democracy and the rule of law in our society.

Extremism is defined in the Counter Extremism Strategy 2015 as the vocal or active opposition to our fundamental values, including the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. We also regard calls for the death of members of our armed forces as extremist"

Under the Counter-Terrorism and Security Act 2015, we have a duty to refer any concerns of extremism to the police (In Prevent priority areas the local authority will have a Prevent lead who can also provide support). This may be a cause for concern relating to a change in behaviour of a child, family member or adult working with the children in the setting, comments causing concern or actions that lead staff to be worried about the safety of a child in their care. Alongside this we will be alert to any early signs in children and families who may be at risk of radicalisation, on which we will act and document all concerns when reporting further.
The NSPCC states that signs of radicalisation may be:
 Isolating themselves from family and friends
 Talking as if from a scripted speech
 Unwillingness or inability to discuss their views
 A sudden disrespectful attitude towards others
 Increased levels of anger
 Increased secretiveness, especially around internet us

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet. The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.
The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet to Jon Willcox.

E-Safety - Roles and Responsibilities

3.1 The local governing body

The local governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The computing lead will oversee online safety.

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.
- 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. Netsweeper – schools broadband – send a report to NTB each week with any searches that are flagged and blocks inappropriate content.

3.3 The designated safeguarding lead

Details of the school's DSL and safe guarding officers are set out in our child protection and safeguarding policy.

The Headteacher/safe guarding officer/Computing Leader (Rachel Spinks), 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 and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged 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
- Liaising with other agencies and/or external services if necessary
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensuring 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.

3.4 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 and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL and computing lead 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.

3.5 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

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

3.6 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:

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

4.2 Curriculum Content - Implementation

- The school believes it is essential for e-safety guidance to be given to the students on a regular and meaningful basis. E-safety is embedded within the curriculum and the school continually looks for new opportunities to promote e-safety.
- The school provides opportunities within a range of curriculum areas to teach about e-safety including, but not limited to, computing and RSHE. Throughout the curriculum, students learn about internet safety and are offered advice on how to stay safe online.
- Pupils are made aware of the dangers when using the internet such as data protection, intellectual property and on-line gaming which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross-curricular teacher models, discussions and via computing.

5. E-safety Skills Development for Staff/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. They also

read and sign the school's Acceptable Use Policy.

- 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).

- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- The Deputy Headteacher/DSL/Computing Leader 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.

6. 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. This policy will also be shared with parents.

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

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.

Parents are sent an online safety newsletter and updates to relevant information in weekly newsletter. Parents are also sent a copy of Ditto online safety magazine which is also saved onto the school website. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Managing the School e-safety Messages

- The School endeavours to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the beginning of each school year.
- There is a dedicated e-safety page on the school website which provides information to parents and pupils, signposts for support, websites etc.

8. Incident Reporting, e-safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to Mr Jon Willcox, Mrs Sarah Keeping and Mrs Rosie Head.

Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must also be reported to the GDPR coordinator, Rebecca Dyball, who will report incidents to GDPR depending on the severity of the breach.

E-safety Incident Log

Minor incidents

- These could include accidental or unintentional access to unsuitable websites, Internet searches which bring up undesirable content or minor misuse IT.
- These should be recorded on the minor incident form in the IT suite and Jon Willcox and Sarah Keeping made aware. The incidents will then be assessed in case further action is needed.

Further Action or More Serious Incidents

- Some incidents may need to be recorded on the Serious Incident Form, particularly if they relate to a bullying or racist incident. Acts of Cyber Crime will be dealt with in accordance with the Computer Misuse Act 1990.
- Jon Willcox and Sarah Keeping must be informed immediately. Further action will then be taken in accordance with CEOP and school safeguarding guidance.

Monitoring of Incidents

- All incidents will be brought to the attention of the senior management team with information on any actions that needed to be taken and how they were resolved.

Orchard Primary School e-safety Incident Log

- Details of ALL e-safety incidents are recorded by Mrs Sarah Keeping. The incident logs will be monitored termly by the Head teacher and Members of SLT.

9. Misuse and Infringements

9.1 Cyberbullying

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 and the anti-bullying policy.)

9.2 Preventing and addressing cyber-bullying

E-safety practice is advocated at all times in school. At St Joseph's School the following will take place:

- 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.

- 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.
- Cyberbullying will be addressed at least termly through assemblies. It will be revisited informally through the year.
- Safer Internet Day will be used to reinforce messages regarding the safe use of technology.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- Information for parents will be put on newsletters and published in the school's website; a meeting for parents to discuss internet safety will be offered annually.
- 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.
- All children, parents and staff sign an Acceptable Use Agreement.
- All incidents of cyberbullying must be reported to the Headteacher and recorded onto CPOMS.
- 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.

Whilst the school recognises that cyberbullying may take place out of school hours, it will wherever possible, step in to mediate a suitable solution.

9.3 Peer on Peer Abuse

This school recognises that children sometimes display harmful behaviour themselves and to others and that such incidents or allegations must be investigated and where appropriate, referred on for appropriate support and intervention.

Such abuse is unacceptable and will not be tolerated.

In the context of this policy, this abuse could for example include:

- 'upskirting'
- all forms of bullying via electronic devices
- aggravated sexting

To prevent peer-on-peer abuse and address the wider societal factors that can influence behaviour, the school will educate pupils about abuse, its forms and the importance of discussing any concerns and respecting others through the curriculum, assemblies and PSHE lessons.

The school will also ensure that pupils are taught about safeguarding, including online safety, as part of a broad and balanced curriculum in PSHE lessons, RSHE and computing.

All staff will be aware that pupils of any age and sex are capable of abusing their peers and will never tolerate abuse as “banter” or “part of growing up”.

All staff will be aware that peer-on-peer abuse can be manifested in many ways, including sexting or cyberbullying which aims to cause emotional or psychological harm, for example.

Pupils will be made aware of how to raise concerns and how any reports will be handled.

If a child has been harmed, is in immediate danger or is at risk of harm, a referral will be made to MASH.

9.4 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, report 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 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:

- 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 and the school's COVID-19 risk assessment.

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

10. 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.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. This is monitored weekly by Netsweeper and a report is sent to Jon Willcox.

11. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during lessons and must give them to the teacher at the beginning of the school day. They are stored securely in the office.

Any mobile devices that are found not handed in will be confiscated and a meeting will be had with parents to discuss further action.

12. 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
- Not sharing the device among family or friends
- 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 Rachel Spinks or Cosmic.

13. 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 computing. 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 or social media policy]. 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.

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every 2 years by the Computing Lead. At every review, the policy will be shared with the local governing board.

15. 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
- Computing

Primary Pupil Acceptable Use Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or offensive. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details, such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer maybe contacted if a member of school staff is concerned about my eSafety.

Signed ……Date……

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, etc is an integral important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like to discuss this further please contact Mr J Willcox.

✂

Parent/ carer signature
We have discussed this and ……(child name) agrees to follow the eSafety rules and to support the safe use of ICT at St Joseph's Catholic Primary School.

Parent/ Carer Signature ……

Class …… Date ……

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, 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 Mr. J Willcox.

- I will only use the school's email / Internet / Intranet / Learning Platform/ (and Tapestry for foundation Staff) and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head 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 will ensure that all electronic communications with pupils and staff are compatible with my professional role.

- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.

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

- I will ensure that personal data 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 Headteacher. Personal or sensitive data taken off site must be encrypted.

- I will not install any hardware or software without permission of the Computing Leader Mrs Sarah Keeping / Mr Jon Willcox.

- 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 without the permission of the parent/ carer, member of staff or Headteacher.

- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.

- I understand that all my use of the Internet and other related technologies (including Tapestry for foundation Staff) can be monitored and logged and can be made available, on request, to my line manager or Headteacher.

- I will respect copyright and intellectual property rights.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute, this includes my use of Facebook and other social media platforms.

- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

- I understand this forms part of the terms and conditions set out in my contract of employment.

- I will follow the prevent duty and report any concerns immediately to the school Designated Safeguarding Lead (Jon Willcox) immediately.

User Signature

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

Signature …….. Date ……

Full Name ……(printed)

Role . . . . . .