St Joseph's Catholic Primary School

Inspiring everyone to REACH through Faith, Hope, Love

At St Joseph's, we strive for academic excellence through encouraging resilience, empathy, aspiration and challenge. We have high expectations for ALL so that we can be 'The best we can be.' With Faith, Hope and Love at the heart of our school family, our children feel safe, secure and supported.

Safeguarding for Technology

(Including E-Safety, Acceptable Usage and Mobile Phone usage)

Our ethos is one that nurtures education through recognition and celebration of all children's experiences and achievements, whatever the context. Each child is unique and made in the likeness of God. Every child should succeed at their own level and be praised for this success

Reviewed by:	Clare Howells
Approved by FGB:	18th January 2023
Review Cycle:	Annually
Next Review Due:	Extended to November 2024 pending LWCET policy

Contents

1. Aims & Scope

At Saint Joseph's Catholic Primary School, we want to ensure that all members of our community are safe and responsible users of technology.

We will support pupils to:

- Become empowered and responsible digital creators and users of technology
- Use our school resources and technology safely, carefully and responsibly
- Be kind online and help us to create a school community that is respectful and caring, on and offline
- Be safe and be sensible online and always know that you can talk to a trusted adult if you need help
- Use devices that have been agreed

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
- Ensure that everyone is safe from the misuse of external devices that are brought in to school

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, antisemitism, 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 scams

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils
- The school has a duty to provide students with quality Internet access as part of their learning experience
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security

How does the Internet benefit education?

- Access to world-wide educational resources including museums and art galleries.
- Cultural, vocational, social and leisure use in libraries, clubs and at home

- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration with support services, professional associations and colleagues
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with the LEA (Local Education Authority) and DfE (Department for Education)
- Access to learning wherever and whenever convenient

How can the Internet enhance learning?

- The school Internet access is designed for pupil use and includes filtering appropriate to the age of pupils
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and ability
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider via the school's ICT technician.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law
- Pupils should be taught to be aware of the materials they read and shown how to validate information before accepting its accuracy
- The evaluation of on-line materials is a part of every subject

How will ICT system security be maintained?

- The security of the school ICT systems will be reviewed regularly by the school's ICT technician
- Virus and ransomware protection will be installed and updated regularly
- Personal data sent over the Internet will be encrypted or otherwise secured
- Use of portable media will be reviewed. Portable media may not be used without specific permission.
- Files held on the school's network will be regularly checked
- The ICT co-ordinator / ICT technician will review system capacity regularly
- Personal external storage devices and CD/DVD's brought in by staff or pupils should not be used without the Head teacher's permission.

How will published content be managed?

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupil's personal information will not be published.
- Email addresses should be published carefully, to avoid spam harvesting
- The Head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright

Can pupil's images or work be published?

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified, without consent
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents. Written consent will be obtained from children's parent or guardian

How will social networking and personal publishing be managed?

- The school will block/filter access to social networking sites
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, e-mail address, names of friends, specific interests and clubs etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. House number, street name, school, shopping centre.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others
- Pupils should be advised not to publish specific and detailed private thoughts
- We are aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments
- The school's computing scheme of work has been extended to incorporate the education of children on the Internet and its safe use – more specifically:
    - Year 6 children take part and engage with the Gloucestershire Police Schools Unit programme – Schoolbeat
    - Reception – Year 5 will take part in the Police Cyber Safety visit to school.

How will filtering be managed?

- Internet Filtering is provided by South West Grid for Learning (SWGfL)
- We will work in partnership with parents, the LEA, DfE, SWGfL and our ICT support provider to ensure systems to protect pupils are reviewed and continually improved
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the ICT technician. Children will be educated as to the correct and safe procedure to do this
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Any material that the school believes is illegal must be referred to the Internet Service Provider.
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate

How should personal data be protected?

The Data Protection Act 2018 (encompassing GDPR) requires that data is**:**

- Processed fairly and lawfully
- Processed for specified purposes

- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures Please refer to the schools GDPR policies available on the school website.

How will Internet access be authorised?

Our pupils' access to the Internet will be by adult demonstration with opportunities for the children to work directly on the Internet individually or with a partner. This will always be directly supervised by a teacher or adult.

How will risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed regularly
- The Head teacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored

How will e-safety complaints be handled?

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Head teacher
- Pupils and parents will be directed to the complaints procedure, which is available on the school website
- Parents and pupils will need to work in partnership with staff to resolve issues
- Discussions will be held with the Police liaison officer to establish procedures for handling potentially illegal issues
- The Safer Internet police agency will be informed of any potentially unsafe practice.
- CEOPs referral may be made if there is a possibility of exploitation e.g. grooming

Sanctions within the school discipline policy include:

- interview / holistic support by the Pastoral Lead / Head teacher;
- informing parents or carers;
- police may be informed;
- removal of Internet or computer access for a period of time.

How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e-safety
- The school will be sensitive to Internet related issues experienced by pupils out of school,

  e.g. social networking sites, and offer appropriate advice

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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. 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.

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).

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 online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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

3.2 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 designated safeguarding lead (DSL) and DDSL's are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working 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.

3.4 The ICT Lead

The ICT Lead 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 monthly 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.

3.5 All staff and volunteers

All staff, including contractors and agency staff:-

- 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/DDSL 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.

All volunteers will sign an= statement to confirm that they understand their responsibilities for online safety.

3.6 Parents

Parents are expected to:

Notify a member of staff, DSL or DDSL 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 resource sheet – Childnet International

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:

All schools have to teach:

- Relationships education and health education in primary schools

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

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

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

The school will raise parents' awareness of internet safety through this policy in letters or other communications home, and in information via our website. This policy will also be shared with parents.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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 1 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. Class Teachers will discuss cyber-bullying with their tutor groups.

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, 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).

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/DDSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL/DDSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

The DfE's latest guidance on searching, screening and confiscation

UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Our behaviour policy

Any complaints about searching for 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 to 3). 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 to 3.

8. Pupils using mobile devices and smart watches in school

In exceptional circumstances – with agreement, pupils may bring mobile devices into school, but are not permitted to use them during the school day. They will be expected to hand them in to the office for safekeeping throughout the day. Phones and smart watches should be clearly marked so that each pupil knows their own phone. Parents are

advised that St Joseph's accept no liability for the loss or damage to mobile phones that are brought into school or school grounds.

9. Staff Responsibilities

9.1 using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure and ensure that work devices must be used solely for work activities.

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 by always installing the latest updates

9.2 General use of technology

Computer network

Obtaining, downloading, sending, printing, displaying, distributing or otherwise transmitting or gaining access to materials which are pornographic, obscene, racist, unlawful, abusive, offensive or inappropriate will be regarded as gross misconduct and will result in disciplinary action.

Staff members must not use any device in any way which would violate the school's online and acceptable usage policy.

If staff have any concerns over the security of their device, they must seek advice DSL/DDSL's

Internet / email

- Use of Gloucestershire County Council (GCC) internet and email must be solely for legitimate school purposes
- Use of the internet and email are subject to scrutiny by the school's filtering provider. Any action that might damage the good reputation of the service will be dealt with as a serious act of misconduct
- Use of the internet for personal financial gain, gambling, political purposes or advertising is forbidden.
- Emails sent from school should contain the same professional levels of language and content as applied to letters or other media
- You are responsible for the email you send and for any contacts you make that might result in inappropriate emails being received

Work Mobile Phones

- Posting anonymous messages and forwarding chain letters is forbidden
- Appropriate security must be used or applied before confidential or sensitive information is sent via the internet or email Mobile phones
- Professional 'voice' to be used in all phone calls made and text messages sent using work phones
- Personal calls, other than in an emergency, are forbidden on work phones

- Calls and contact to parents / carers should be restricted to the hours of 8.00am to 6.00pm and only using school telephones or mobile phones. An exception may be made in the case of a residential trip in order to inform parents of safety or important information

Social Media

- Staff must not share their personal contact details Social Media Social media is used increasingly across society and is recognised as a hugely valuable communication tool. However, the open nature of the internet means that social networking sites can leave professionals vulnerable if they fail to observe precautions. This policy is designed to protect staff and pupils from potential harm or from becoming victims of radicalisation, extremism and malicious, upsetting or inadvisable contact. Please refer to Child Protection and Safeguarding Policies available on the school's website.
- All staff must avoid contacting pupils on social networking sites. This is to avoid any possible misinterpretation of motives and the risk of any allegations being made. Pupils must not be added to social media sites for staff.
- Staff social media networks e.g. Facebook, Instagram, Twitter, Snapchat etc must not be used in any way which can bring the school into disrepute; this will be dealt with as an act of misconduct
- Staff members must not identify themselves as employees of the school in their personal web space. This is to prevent information on these sites from being linked with the school and Page 4 of 6 the County Council and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services
- Staff members must not make contact through any personal ICT or social medium with any pupil, whether from our school or any other school unless the pupil is your own family member OR an existing close family friend.
- Staff must not have social media contact with any pupils' family members / carers. This is in line with NASUWT teachers' union and other unions. Teachers should not, for example, accept Facebook requests from parents of a pupil.
- Staff members must decline friend requests from pupils.
- On leaving school employment, staff members must not contact pupils by means of social media accounts.
- Any information staff members have access to as part of their employment, including personal information about: pupils and their families, colleagues, County Council staff and other parties must not be discussed on their personal webspace or social media sites.
- Photographs, videos or any other types of images of pupils and / or their families or images depicting staff members who can be identified as school staff members must not be published on personal web space or social media sites.
- School or County Council email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.
- Staff members must not edit open access encyclopedias such as Wikipedia in a personal capacity at work. This is because the source of correction will be recorded as the school's IP address.
- School logos or brands must not be used or published on personal web space / social media sites.
- School does not permit personal use of social media or the internet during core contracted hours, both within school and on visits.
- Caution is advised when inviting work colleagues to be 'friends' on personal networking sites. Social networking blurs the line between work and personal lives.
- Staff must not use social media and the internet in any way to attack, insult, abuse or defame: pupils, their family members. Colleagues, other professionals, other organisations, School or County Council - either openly or by suggestion.
- Staff members are strongly advised to set the privacy levels of their personal social media sites as strictly as they can and to opt out of public listings in order to protect their own privacy. Staff members should keep passwords confidential, change them often and be cautious about what is posted online. Staff are advised to take all precautions to avoid identity theft.

9.3 Personal phone and smart watch usage at work

Staff use of mobile phones or smart watches during their working day should be:

- outside of their contracted hours
- discreet and appropriate (not in the presence of pupils or in areas where pupils may walk through)

Mobile phones should be switched off and left in a safe place during lesson times. The school cannot take responsibility for items that are lost or stolen.

Staff should never contact pupils or parents from their personal mobile phone or give their mobile phone number to pupils or parents. If a member of staff needs to make telephone contact with a pupil, they should use the school telephone in the office. In some circumstances, staff will have the school internet phone app downloaded. Where this is agreed, phone calls can be made on their personal devices this app.

Staff should never send to, or accept from, colleagues or pupils, texts or images that could be viewed as inappropriate.

With regard to camera phones, a member of staff should never use their phone to photograph a pupil(s) or allow themselves to be photographed by pupils.

This guidance should be seen as a safeguard for members of staff, the school and the Local Authority. Staff should understand that failure to comply with the policy is likely to result in the enforcement of the Whistleblowing policy and associated procedures.

10. Parents/carers, visitors and volunteers

Adults either in school or accompanying children on school trips should not use any devices to take pictures of pupils unless it is at a public event such as Sports day or Summer fair and of their own children.

Adults, visitors or volunteers in school should only use their mobile phone within the confines of the school office or staff room. Personal cameras and mobile phone cameras should not be used to take pictures of children. If parents who accompany children on a school trip are asked by the teacher to take photos as a record of the educational visit, they will be issued with a school device. Parents accompanying children on school trips should not use their mobile cameras or any other device to take pictures of children.

11. How the school will respond to issues of misuse -

By Pupils:-

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and online/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 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.

Where a pupil is found by a member of staff to be using a mobile phone or smart watch, the device will be confiscated from the pupil, handed to a member of the office team who will record the name of the pupil and attach it to the phone. The devise will be stored by the school office for the pupil's parent or carer to collect.

If a pupil takes photographs or video footage with a mobile phone or smart watch of either other pupils or teachers, action will be taken accordance to our Behaviour policy. If images of other pupils or teacher have been taken, the phone will not be returned to the pupil until the pupil in the presence of the Acting Head Teacher or SLT has removed the images.

If a pupil uses their phone inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able to bring a phone into school.

Should parents need to contact pupils or vice versa during the school day, this should be done via the usual school procedure of contacting the school office via phone or email.

By Staff:-

- Any breach of this policy may be investigated and may lead to disciplinary action being taken against the staff member/s involved. This is in line with the School Disciplinary Procedure.
- A breach of this policy leading to breaches of confidentiality or defamation or damage to the reputation of the school or any illegal acts or acts that render the school or County Council liable to third parties may result in disciplinary action or dismissal
- Contracted providers of the school must inform the county Council officer immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the service and the County Council. Any action against breaches should be according to contractors' internal disciplinary procedures. Please see GDPR policy and associated Policies.

12. Training

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

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

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

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

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

The DSL and DDSL 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.

13. Monitoring arrangements

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

This policy will be reviewed every year by the DD 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.

14. 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

Keeping Children Safe in Education 1St September 2022– Annex D

Appendix 1

St Joseph's Catholic Primary School

Diocese of Clifton

Inspiring Everyone to REACH through Faith, Hope, Love

Front Street, Nympsfield, Stonehouse, Gloucestershire GL10 3TY
Telephone/Fax No: 01453 860311 Email: SLT@st-josephs.gloucs.sch.uk
Website: www.st-josephs-nympsfield.com

Headteacher: Mrs Clare Howells

Mobile Phone Parental Consent Form

Dear Parent/Carer

In accordance with our mobile phone policy, if your child is bringing in a mobile phone to school, please sign the form below to give your permission for your child to do this and remind them of our school policy.

- Your child needs to bring their phone to the school office first thing in the morning before they go their classroom.
- The school bears no responsibility for the loss or damage to a mobile phone.
- Your child's phone should be appropriately marked so that they can recognise it.
- Should your child be found using their phone inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able to bring their phone into school.

Yours sincerely

Clare Howells
Head teacher

……

MOBILE PHONE PARENTAL CONSENT

I/we give permission for our child (name) …… in Year ……..

to bring their mobile phone into school.We have read the policy and understand its implications

Signed …….. Date……..

PRIVACY NOTICE: Please note; we are collecting the personal information you provide above to enable us to maintain an accurate record of your consent and understanding of this mobile phone policy. This information is protected under our GDPR policies and Privacy Statement. Please see the school website or ask at the school receptions if you would like to know more.

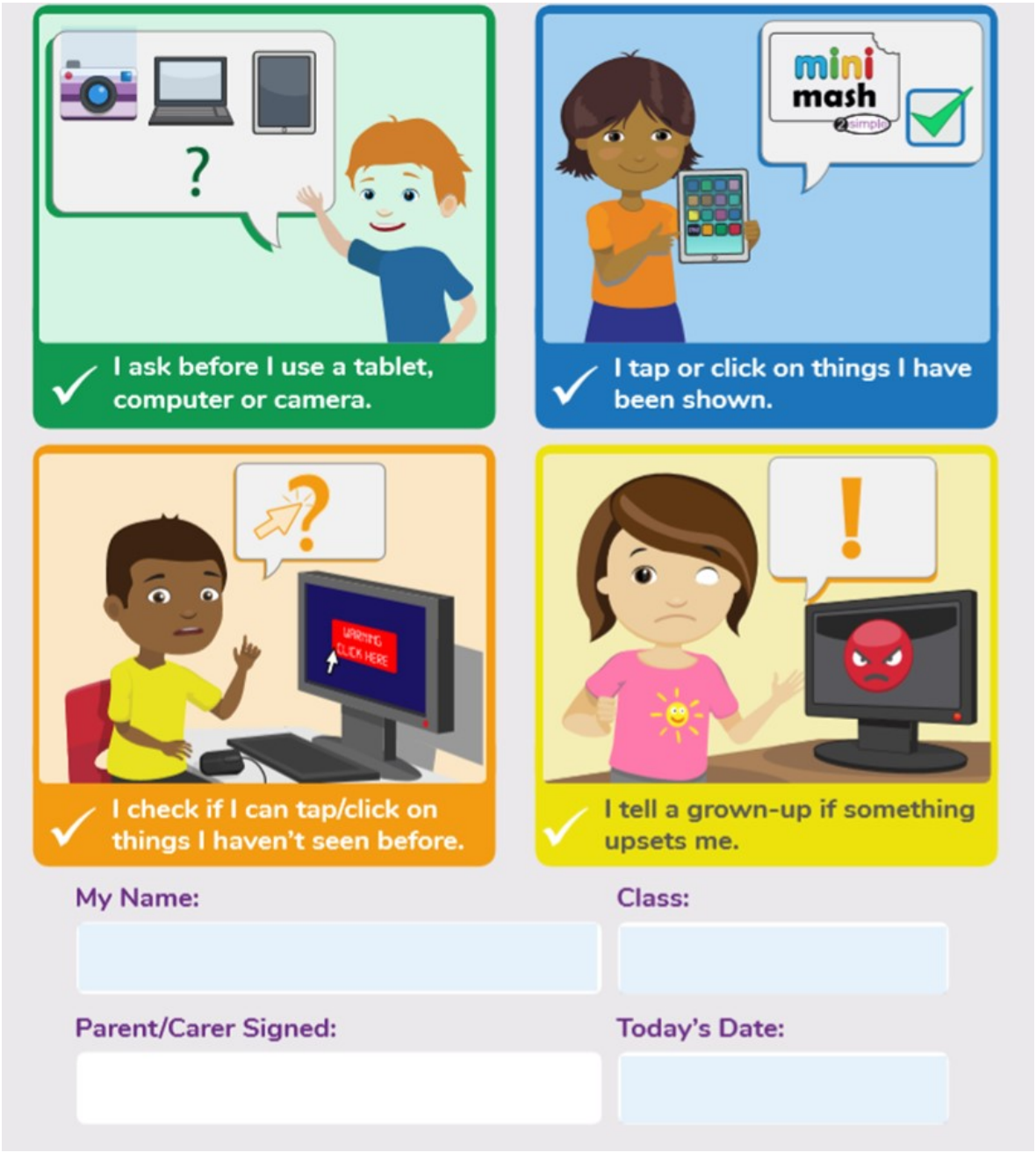
PLEASE RETURN PERMISSION SLIP TO THE SCHOOL OFFICE. THANK YOU.

Appendix 2a: acceptable use agreement EYFS (pupils and parents/carers)

St Joseph's Catholic Primary School

Inspiring everyone to REACH through Faith, Hope, and Love

Acceptable Use Agreement (EYFS)



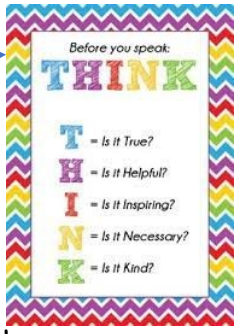
Appendix 2b: acceptable use agreement KS1 & KS2 (pupils and parents/carers)

St Joseph's Catholic Primary School

Inspiring everyone to REACH through Faith, Hope, and Love

Acceptable Use Agreement

- ✓ I will only access computing equipment when a trusted adult has given me permission and is present.
- ✓ I will not deliberately look for, save or send anything that could make others upset.
- ✓ I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- ✓ I will keep my username and password secure; this included not sharing with others.
- ✓ I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- ✓ I will always use my own username and password to access the school network and subscription series such as Times Table Rockstars.
- ✓ In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact me parents/carers if an adult at school is concerned about me.
- ✓ I will respect computing equipment and will immediately notify and adult if I notice something isn't working properly or is damaged.
- ✓ I will use all communication tools such as emails carefully. I will notify an adult immediately if I notice that someone is using a computer/phone/smartwatch.
- ✓ Before I share, post or reply to anything online I will T.H.I.N.K.
- ✓ I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.



I understand this agreement and the consequences if I don't follow it.

Name

Signature of parent/carer

Date

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

St Joseph's Catholic Primary School

Inspiring everyone to REACH through Faith, Hope, and Love

Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET AND SOCIAL MEDIA: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

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

- ✓ Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- ✓ 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, or connect unauthorised hardware or devices to the school's network
- ✓ Share my password with others or log in to the school's network using someone else's details
- ✓ Take photographs of pupils without checking with teachers first
- ✓ Share confidential information about the school, its pupils or staff, or other members of the community
- ✓ Access, modify or share data I'm not authorised to access, modify or share
- ✓ Promote private businesses, unless that business is directly related to the school

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 the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

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 policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager 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.

I will follow the guidelines set out within this policy with regards to my own personal use of IT.

Signed (staff member/governor/volunteer/visitor): **Date:**

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
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, volunteers, governors 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 cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

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**