

St. Joseph's Catholic Primary School

Online safety Policy

Here at St Joseph's Catholic Primary School, we learn and grow through the love of Jesus. Our community is a safe, caring and happy place where everyone is supported and valued. We encourage and challenge everyone to achieve their full potential, spiritually, academically, morally and socially. We inspire others with a love of learning and aim for excellence in everything we do. Through our own faith, we treat one another the way we would like to be treated. We help every child to be gentle and fair: to always do their best.

'Learning through the Love of Jesus Christ'

Introduction

Here at St Joseph's we are committed to giving all of our children every opportunity to achieve the highest of standards. We offer a broad and balanced curriculum and have high expectations of all the children. The achievement, attitude and well-being of all our children matter. This policy helps to ensure that this school protects and promotes the individual, irrespective of ethnicity, attainment, age, disability, gender or background. We do this by taking account of pupils' varied needs.

St Joseph's is committed to providing a safe and secure environment for its pupils and staff. The governors and staff are committed to promoting British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths, cultures and lifestyles.

This policy should be read in conjunction with the school's Safeguarding and Child Protection Policy, Behaviour Policy and Safer Internet use agreement.

The School Online Safety Coordinator is Mandy Nash
The governor with responsibility for online safety is Mrs Joan McConnell

Teaching and learning

Why is Internet use important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- 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 need to learn how to evaluate internet information and to take care of their own safety and security.
- 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 functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;

St. Joseph's Catholic Primary School

Online safety Policy

- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online 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.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems

How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

How will email be managed?

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole class or group email addresses will be used in primary schools for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Staff should not use personal email accounts during school hours or for professional purposes.
- The forwarding of chain messages is not permitted.
- Access in school to external personal email accounts may be blocked.

St. Joseph's Catholic Primary School

Online safety Policy

How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupils' images or work be published?

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- 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 images/videos of pupils are electronically published.
- Pupils work can only be published with their permission or the parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.

How will social networking, social media and personal publishing be managed?

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.
- Parents are advised that they should be aware of the risks from uploading images of their children on social media sites.
- Any pictures taken in school during assemblies or plays should not be uploaded for any reason.
- Parents helping on trips are treated as volunteer staff and as such have signed an agreement that clearly states that they are not allowed to take photos of the children. (See guidance on volunteer staff on school trips)

St. Joseph's Catholic Primary School

Online safety Policy

How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with LGfL team to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Online Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Police or CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.

How should personal data be protected?

St Josephs processes personal data about its pupils and is a "data controller" in respect of the Data Protection Act 1998.

St Joseph's Catholic Primary School processes data to:

- Support it's pupils learning
- Monitor and report their progress
- Provide appropriate pastoral care and assess how well the school is doing as a whole

This data includes contact details, national curriculum assessment results, attendance information, ethnic group, SEN and medical information. St. Joseph's is required to share this information with the Local Authority, DCSF, QCA, Ofsted etc. We also share information through SIMS which is part of the school office computer system. All of these organizations are data controllers and are subject to the same legal constraints in how they deal with the data.

Policy Decisions

How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitor to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

Date: March 2017

Date of next review: September 2018

St. Joseph's Catholic Primary School

Online safety Policy

- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- In Foundation Stage and KS1, pupils access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor LGfL can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Bromley Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The Online Safety Coordinator will record all reported incidents and actions taken.
- The Designated Child Protection Coordinator will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage Online Safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team and escalate the concern to the Police.

How will e-Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All Online Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How is the Internet used across the community?

Date: March 2017

Date of next review: September 2018

St. Joseph's Catholic Primary School

Online safety Policy

- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's Online Safety ethos.
- Sanctions for those involved in cyberbullying may include:
- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

How will a sexting/nude selfie incident be managed:

[UKCCIS "Sexting in schools and colleges"](#) should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or people
- Why was the imagery shared?
- Was the young person coerced or put under pressure to produce the imagery?
- Who has shared the imagery?
- Where has the imagery been shared?
- Was it shared and received with the knowledge of the pupil in the imagery?
- Are there any adults involved in the sharing of imagery?
- What is the impact on the pupils involved?
- Do the pupils involved have additional vulnerabilities?
- Does the young person understand consent?
- Has the young person taken part in this kind of activity before?
- If a referral be made to the police and/or children's social care.
- Is it necessary to view the imagery in order to safeguard the young person (in most cases, imagery should not be viewed).
- What further information is required to decide on the best response.
- Whether the imagery has been shared widely and via what services and/or platforms (This may be unknown).

St. Joseph's Catholic Primary School

Online safety Policy

- Whether immediate action should be taken to delete or remove images from devices or online services.
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual.
- Whether to contact parents or carers of the pupils involved (in most cases parents should be involved).

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example young person with special educational needs or disability)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then we may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

How will mobile phones and personal devices be managed?

- Mobile phones and personal devices are not permitted to be used in school by pupils.
- Any pupil bringing a mobile phone or personal device to school must hand it in to the school office until the end of the day. Any pupil found with a mobile phone during the school day will have it confiscated until the end of the day.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Communication Policy

How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.
- An Online Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.

Date: March 2017

Date of next review: September 2018

St. Joseph's Catholic Primary School

Online safety Policy

- An Online Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- Online Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- Online Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to Online Safety education will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

- The Online Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school Online Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to Online Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting Online Safety at other attended events e.g. parent evenings and sports days.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss it's implications with their children.
- Information and guidance for parents on Online Safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in the "Online Safety Contacts and References section".

Online Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre):

www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Bromley Children's Safeguarding Team 02084617309

Children's Safeguards Team: <http://www.bromleysafeguarding.org/index.asp>

Click Clever Click Safe Campaign: <http://clickcleverclicksafe.direct.gov.uk>

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Metropolitan Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Metropolitan Police via 101.

Kidsmart: www.kidsmart.org.uk

LGfL: www.lgfl.net

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce – Report Abuse: www.virtualglobaltaskforce.com