St Joseph's Catholic Primary School, Pontefract
A Voluntary Academy

E-Safety Policy 2019-2021

Date of publication: September 2019 Review date: September 2021

St Joseph's Catholic Primary School,
Newgate,
Pontefract
WF8 4AA

Tel: 01977 701493
Email: admin@sjp.bkcat.co.uk

Headteacher: Mrs Michaela Velayudhan Tomlin
IT Leader: Mr Ben Sandbach

Our Mission

Here, under the guidance of our patriarch,
St Joseph, and inspired by centuries of
Catholic teaching, we begin to learn how
to serve each other and our world with
the same faithful joy which we see in
Jesus, our saviour and our Lord.

To Him be glory and praise for ever

Introduction

St Joseph's Catholic Primary School, fully recognises the contribution it can make to protect children and support them in school. The aim of this policy is to safeguard and promote our pupils' safe use of internet and electronic communication technology such as mobile phones and wireless connectivity.

This policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school.

It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

The school e-safety policy will operate in conjunction with others including policies for Behaviour, Safeguarding, Anti-Bullying, Equal Opportunities and Internet Access Agreement with parents/carers.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible IT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband;
- A school network that is compliant with National Education Network standards and specifications.

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for IT, anti-bullying and for Safeguarding/Child protection.

The school has appointed Mr B. Sandbach as e-Safety Coordinator.

- Our e-Safety Policy has been written by the school, building on the LA e-Safety Policy, and government guidance. It has been agreed by senior management and approved by governors.

Teaching and learning

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access has been designed expressly for pupil use and includes filtering appropriate to the age of pupils. The IT technicians, through discussion with the Headteacher and IT Co-ordinator ensure this is kept up to date.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- 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 shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

Managing Internet Access

Information system security

- School IT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will follow LA & Trust guidance.

E-mail

- At the moment we have no procedures in school where children use email

Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that they are appropriate for use on a social network.
- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or work of pupils is published on the school website.
- Work published on the website will not be identified with an individual pupil.
- Pupil image file names will not refer to the pupil by name.

- Parents/carers are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Sites such as MSN and Build a Bear etc. should **NOT** be used.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Managing filtering

- The school will work with their chosen technicians to ensure systems to protect pupils are reviewed and improved continuously.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator/IT support.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing & webcam use

- Video conferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior management team are aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during school time. The sending of abusive or inappropriate text messages or files by Internet, Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will not be allowed (but kept under review in light of changing advances in technology).
- Staff will use a school phone where contact with pupils is required.
- The appropriate use of the Website / VLE / Learning Platforms will be discussed as the technology becomes more widely used within the school.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the **Data Protection Act 2018** (the UK's implementation of the General **Data Protection** Regulation or GDPR)

Policy Decisions

Authorising Internet access

- All staff must read and sign the BKCAT acceptable use of IT and the BKCAT code of conduct, before using any school IT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved, on-line materials.
- An 'acceptable use policy' - for school IT resources, is required to be agreed to by all users, before accessing the school IT network.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor the BKCAT can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

Communications Policy

Introducing the e-safety policy to pupils

- E-Safety rules will be posted in the ICT suite and in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed within school.
- E-Safety training will be and is, embedded within the IT scheme of work.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor IT use will be supervised by senior management and work to clear procedures for reporting issues.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school website.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

Ensuring that our children have every opportunity to develop the confidence and capacity to become successful, lifelong learners is a key task for us.
St Joseph's is a school committed to Growing, Learning, Achieving Together with strong Catholic values underpinning this.

The following policy statement is split into two parts;

a- Staff use of Social networking sites.
b- Parents use of social networking sites.

This policy does not deal with child use of social networking sites. This is detailed in our e safety policy.

SOCIAL NETWORKING
STAFF USE OF SOCIAL NETWORKING SITES.

Introduction

Social networking activities conducted online outside work, such as blogging (writing personal journals to publicly accessible internet pages), involvement in social networking sites and posting material, images or comments on sites such as You Tube can have a negative effect on an organisation's reputation or image. In addition, St Joseph's has a firm commitment to safeguarding children in all aspects of its work. This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.

Key Principles

- Everyone* at St Joseph's has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.

- It is important to protect everyone* at St Joseph's from allegations and misinterpretations which can arise from the use of social networking sites.

- Safeguarding children is a key responsibility of all members of staff and it is essential that everyone* at St Joseph's considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with children from our school via social networking.

- This policy relates to social networking outside work. Blogging and accessing social networking sites at work using school equipment is not permitted.

- No communications irrespective of their anonymity should be shared that relate to any specific event, protocol, pupil or person at St Joseph's School.

Code of Conduct for Everyone* at St Joseph's – Social Networking

The following are **not considered acceptable** at St Joseph's School:

- The use of the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material including the internet or written documentation.

*In the context of this policy "everyone" refers to members of staff, governors, Friends and anyone working in a voluntary capacity at the school

- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.

- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.

- The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.

In addition to the above everyone* at St Joseph's School must ensure that they:

- Do not use social networking sites to make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.

- Use social networking sites responsibly and ensure that neither their personal/professional reputation, or the school's reputation is compromised by inappropriate postings.

- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.

Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.

- The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

*Staff are asked to sign the agreement in the appendix.

B-PARENTS' USE OF SOCIAL NETWORKING SITES

If the staff or governors become aware that there is inappropriate* material about school, staff or pupils published via social networking sites we will follow these procedures;
(By inappropriate we refer to any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.)

1. Print copies of the screen for evidence if possible. A screenshot of the comment or page makes it much easier to deal with the problem and ensures that you are not put in the difficult position of having to believe or disbelieve someone if at a later date the entry is changed or deleted.

2. If the incident involves a child being at immediate risk or the message/picture is of an inappropriate nature e.g. bullying
    a. Inform the Designated Child Protection Coordinator and follow schools' child protection procedures,
    b. Contact Safeguarding and Family Support, 01977 727037.

3. Contact the police if the material posted is illegal – e.g. advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin.

4. In the first instance the easiest solution is often to contact the parent/carer involved and arrange a meeting with them unless it is a potential safeguarding issue and family could be involved.
    a. At the meeting you may wish to discuss the problem and remind them of the school's policy for dealing with complaints.
    b. You may also wish to ask the parent/or child to remove the comment/post at this time.
    c. If the parent/carer proves to be difficult and refuses then you may wish to involve the local community support officer.

5. Involve the community police officer as they may be a good person to approach people outside the school community posting material particularly if the material is grossly offensive, menacing character or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety.

6. Report the abuse via the Facebook site using the report abuse facility (see appendix). For support, if appropriate, contact your ICT support service or School Improvement Business Support Team on 01977 722510.

7. During or after dealing with the incident consider sending a letter to all members of the school community reminding them of the schools complaint procedures and anti-bullying policy.

Parents posting unwanted/offensive comments about the school/staff/pupils

Typical scenario

A parent makes you aware that other parents are posting disparaging comments about a teacher in school.

A member of the school community shows you a screenshot from a parent's profile that has upsetting comments about a child in your school.

Information

Schools are increasingly finding that many problems related to Facebook involve parents/carers posting inappropriate comments about the school, members of staff and in some cases other pupils. Often the first that a school may know of this is when a screenshot is handed to a member of staff or someone inadvertently stumbles upon it. A simple internet search with your school name and the word Facebook can throw up a number of pages that you may not be aware of. For users registered on Facebook you can search your school name and filter by pages, people, public posts etc.

Immediate action: Dealing with an offensive post/comment

Regardless of whether it is an offensive post on a public or private wall or a page that has been created once you have physical evidence you are in a much stronger position to deal with the issue. A screenshot of the comment or page makes it much easier to deal with the problem and ensures that you are not put in the difficult position of having to believe or disbelieve someone.

In the first instance the easiest solution is often to contact the parent/carer involved and arrange a meeting with them. At the meeting you may wish to discuss the problem and remind them of the school's policy for dealing with complaints. You may also wish to ask the parent to remove the comment/post at this time. If the parent/carer proves to be difficult and refuses then you may wish to involve the local community support officer. A number of legal safeguards exist that can be used to support this.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

If you do not have access to a screenshot then you will need to ask the person reporting the issue to provide one. If this is not possible the situation can be slightly more complex to resolve as you have no 'evidence' of the problem. In this instance you should treat the problem in the same way that you would if you had been made aware that parents were 'grumbling' on the playground.

If the comments have been made about a particular member of your school community e.g. a teacher you will need to offer them support as they may be feeling very upset and vulnerable. They may need additional support from a colleague or in some cases from an external agency such as the Teacher Support Network.

Preventative strategies

It is important to ensure that your Anti-bullying policy is up-to-date and includes information on school procedures for dealing with cyberbullying of staff and pupils. Any anti-bullying policy should set out clear disciplinary sanctions for cyber bullying and specify the member of staff to whom incidents of cyber bullying should be reported. You may wish to include a flow chart diagram which explains how the issue will be dealt with. A member of the senior leadership team should be designated to deal with cyber bulling issues and should receive training in new technologies, the possible dangers and how to deal with them. Ensure that all staff are aware of how to report issues and that any issues are logged appropriately.

After dealing with the incident consider sending a letter to all members of the school community reminding them of the school stance on cyberbullying, as part of this you may wish to invite parents/cares to an awareness raising session.

You may also like to run some awareness raising sessions with your pupils on cyberbullying. There are a number of short films that can be used to illustrate the impact of cyberbullying and include lesson plans and resources for follow-up work.

Appendix 1: Useful resources

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org/

Kidsmart
www.kidsmart.org.uk/

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Family Online Safe Institute
www.fosi.org

Internet Safety Zone
www.internetsafetyzone.com

Appendix 2:

St Joseph's Catholic Primary School, Pontefract.

ACCEPTABLE INTERNET USE STATEMENT

Parents/Guardians of pupils should sign a copy of this Acceptable Internet Use Statement and return it to the school where it will be countersigned by a member of staff. Failure to read and complete this form will restrict the use of the computers in school for your child. ***Thank you for your co-operation.***

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school has an Internet Access Policy drawn up to protect all parties - the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

- Access should only be made via the authorised account and password that should not be made available to any other person.
- The security of the IT system must not be compromised whether owned by the Trust, school, by the LA or any other organisation or individual.
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- Users are responsible for all e-mail and messages sent and for contacts made that may result in e-mail being received.
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.
- Posting anonymous messages and forwarding chain letters is forbidden.
- **Cyber bullying, using abusive and unkind comments is forbidden.**
- Copyright of materials and intellectual property rights must be respected.
- All Internet use should be appropriate to staff professional activity or to student's education.

However please note that:-

- ➢ The school's IT system may be used for private purposes following guidelines established by the Trust and school.
- ➢ Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- ➢ Closed discussion groups can be useful but the use of public chat rooms is not allowed.
- ➢ Pupils' irresponsible use of the internet will result in temporary/permanent exclusion of use.

Members of staff are reminded that they should not deliberately seek out inappropriate/offensive materials on the Internet and that they are subject to the Trust/LA's recommended disciplinary procedures should they do so.

Child's name ______________________

Signed ______________________ date ________________
(parent/guardian)

Approved ______________________ date ________________
(Head/class teacher)

Appendix 3:

St Joseph's Catholic Primary School, Pontefract.

Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning.

These rules will keep everyone safe and help us be fair to others.

- **I will use only my own login and password, which I will keep secret.**
- **I will not access other people's files.**
- **I will use the computers only for schoolwork and homework.**
- **I will not bring memory sticks/disk drives into school.**
- **I will ask permission from a member of staff before using the Internet;**
- **I will only e-mail people I know, or my teacher has approved;**
- **The messages I send will be polite and sensible; I will not email anyone or send messages electronically using abusive, inappropriate or unkind comments.**
- **I will not give my home address or phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;**
- **I will not give out personal contact details on line or post photographs of myself on sites.**
- **To help protect other pupils and myself, I will tell a teacher or other adult if I see anything I am unhappy with or I receive a message I do not like; I will not respond to abusive emails.**
- **I understand that the school can check my computer files and the Internet sites I visit.**

Appendix 4:

St Joseph’s Catholic Primary School, Pontefract.

Staff Code of Conduct for IT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school’s e-safety policy for further information and clarification.

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

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

- I understand that school information systems may not be used for private purposes without specific permission from the headteacher.

- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.

- I will not install any software or hardware without permission.

- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children’s safety to the DSL.

- I will ensure that electronic communications with pupils/parents/carers including email and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school’s information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school’s information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.