St. Joseph's
Catholic Primary School

School Internet Policy and E-Safety Guidelines

We follow in Jesus' footsteps, as we care for each other when we work, play and pray.

At St. Joseph's Catholic Primary School we recognise that all children have rights as outlined in the UN Convention. As duty bearers, we have the responsibility to respect these rights and are committed to supporting our children through their education and to ensure that they are rights-holders.

We aim to provide our pupils with their 'right to find out things and share what you think with others by talking, drawing, writing or in any other way unless it harms or offends other people' as stated in Article 13
The right to 'get information that is important to your well-being from radio, newspaper, books, computers and other sources. Adults should make sure that the information you are getting is not harmful and help you find and understand the information you need' as stated in Article 17
The right to 'be protected from being hurt and mistreated, in body or mind' as stated in Article 19.

Introduction:

At St Joseph's we believe that the Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. This school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them. This document sets out the policy and practices for the safe and effective use of the Internet in St Joseph's Primary school. The policy and its implementation will be reviewed annually.

Our Vision

St. Joseph's Catholic Primary School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and children to unacceptable risks and dangers. To that end, St. Joseph's Catholic Primary School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

How will Internet use enhance learning?

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what is acceptable and what is not acceptable 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 maturity. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.

How does the Internet benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- Access to the school website.
- educational and cultural exchanges between pupils world-wide; cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and children while on the school premises.

Related Documents:

Acceptable Use Policy (AUP) for Adults and Young People - Internet and associated communications technologies, Computing Policy, Data Protection Policy, Behaviour Policy, Anti-bullying Policy, Whistle blowing Policy, Safe Guarding Policy,

Publicising e-Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens.

To achieve this we will:

- Make this policy, and related documents, available on the school website at: www.stjosutton.net
- Introduce this policy, and related documents, to all stakeholders (Staff, parents, pupils, governors) at appropriate times.
- Post relevant e-Safety information in all areas where computers are used
- Provide e-Safety information to parents through the website and school newsletters.

Roles and Responsibilities

The Principal and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our school.

The role of e-Safety co-ordinator has been allocated to Miss Olivia Harris under the direction of the Principal. Our DSL (Designated Senior Person) for Safeguarding is the Vice Principal Mrs Natalie Hill and a member of the SLT.

The e-Safety co-ordinator is the central point of contact for all e-Safety issues and will be responsible for day to day management. The school an IT network manager, Mr S Rice and an IT group across the MAC that considers e-Safety that are responsible for policy review, risk assessment, and e-safety in the curriculum.

Pupil views are also considered and fed back to the Principal through the use of the School Council.

All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the e-Safety coordinator using the school procedures
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action.

Additional roles and responsibilities are discussed in the Acceptable Use Policy: Establishing safe and responsible behaviours and Physical Environment / Security.

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor access to the system consulting with the MAC where appropriate. Anti-virus software is installed on all computers and updated regularly

Central filtering is provided and managed by the MAC IT team. All staff and students understand that if an inappropriate site is discovered it must be reported to the e-Safety co-ordinator who will report it to the IT Team to be blocked. All incidents will be recorded in the e-Safety log for audit purposes.

Pupils use is monitored by staff who are always present.

Staff use is monitored by the Principal/e-safety co-ordinator/ IT Team.

All staff are issued with their own username and password for network access. Visitors / Supply staff are issued with temporary ID's and the details recorded in the school office

Key stage one pupils use class logon ID's for their network access

Key stage two pupils have their own username and password and understand that this must not be shared

Code of Safe Practice:

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity.

The scope of the Code covers fixed and mobile Internet; school PCs, laptops, and digital video equipment.

The ICT Technician will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

Code of Practice for pupils:

Pupil access to the Internet is through a filtered service, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Parental permission is sought from parents on entry to the school, before pupils access the internet.

In addition, the following key measures have been adopted by St Joseph’s to ensure our pupils do not access any inappropriate material:

- The school’s Responsible computer/internet use and other digital technologies is made explicit to all pupils and is displayed prominently (see appendix).
- Our Code of Practice is reviewed each school year and signed by pupils/parents on the reverse of the Contact forms (retained in the main office).
- Pupils using the Internet will normally be working in highly-visible areas of the school.
- All online activity is for appropriate educational purposes and is supervised, where possible.

- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group.
- Pupils are educated in the safe and effective use of the Internet, through a number of selected programmes.
- An e-safety curriculum is in place and delivered to the children across all key stages.

During school hours pupils are forbidden to play computer games or access social networking sites, unless specifically assigned by the teacher.

Code of practice for staff:
Staff have agreed to the following Code of Safe Practice:

- Pupils accessing the Internet should supervised by an adult at all times.
- All pupils are aware of the rules for the safe and effective use of the Internet. These are displayed in classrooms and discussed with pupils.
- All pupils using the Internet have written permission from their parents.
- Recommended websites for each year group are available under Favourites. Any additional websites used by pupils should be checked beforehand by teachers to ensure there is no unsuitable content and that material is age-appropriate.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the SLT.
- In the interests of system security staff passwords should only be shared with the network manager.
- Photographs of pupils should always be taken with a school camera and images should be stored on a centralised area accessible only to teaching staff and the network manager.

Mobile / emerging technologies
All staff understand that the Acceptable Use Policies apply to all equipment at all times both off and on site.
To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network.
Staff understand that they should use their own mobile phones sensibly and in line with school policy.
St. Joseph's Catholic Primary School discourages pupils from bringing mobile phones to school due to the potential issues of bullying or harassment directed against pupils and teachers. When a child needs to bring a phone into school, a permission slip must be signed by their parent (See mobile phone policy) and the mobile phone must be left in the school office at the start of the day and collected at the end of the day. The Educations and Inspections Act 2006 grants the Principal the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Principal will exercise this right at their discretion
Pictures / videos of staff and pupils should not be taken on personal devices.
New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community.

E-mail
The school e-mail system is provided, filtered and monitored by Link2ICT / IT team and is governed by the STJPIIMAC.
All staff are given a school e-mail address and understand that this must be used for all professional communication.
Key stage one pupils have access to class based e-mail accounts that are monitored by the class teacher.
Keys stage two pupils are given a school e-mail address that can be used for class based activities
Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication.

Guidance is given to the school community, through staff training days and taught lessons, around how e-mail should be structured when using school e-mail addresses.
Staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with e-mail procedure. In addition, they also understand that these messages will be scanned by the monitoring software
Pupils may be given the opportunity to check their own e-mail outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software.

Everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher / e-Safety co-ordinator as soon as possible.
St. Joseph's encourages all staff and pupils to change their passwords regularly to enhance security.

Published content
The Principal takes responsibility for content published to the school web site but delegate's general editorial responsibility to the staff.
The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.

The school encourages the use of e-mail to contact the school via the school office / generic e-mail addresses / staff e-mail addresses.
The school does not publish any contact details of the pupils

Digital and Video Images of Pupils:
Parental permission is sought at the start of each school year to cover the use of photographs of pupils on the school website, in the local press and for displays etc within school and written permission must be obtained from parent/carer.

School Website:
Our school website promotes and provides up to date information about the school, as well as giving pupils an opportunity to showcase their work and other aspects of school life. In order to minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken:

- Group photos are used where possible, with general labels/captions;
- Names and images are kept separate – if a pupil is named their photograph is not used and vice-versa;
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.

Storage of images:
Digital and video images of pupils are, where possible, taken with school equipment. Images are stored on a centralised area or School Website, accessible only to teaching staff and the network manager.

Digital Media
We respect the privacy of the school community and will obtain written permission from staff, parents, carers, governors or pupils before any images or video are published or distributed outside the school.
Photographs will be published in line with Becta guidance and not identify any individual pupil.
Students' full names will not be published outside the school environment.
Students understand that they must have their teachers' permission to make or answer a video conference call.
Supervision of video conferencing will be appropriate to the age of the pupils.
When pupils leave the educational setting staff will endeavour to remove all digital images from the school website within one year of them leaving, unless written permission is granted from parents.

Social Networking and online communication
The school is reviewing the use of social networking sites and online communication and currently does not allow access to these.
Guidance is provided to the school community on how to use these sites safely and appropriately. This includes:

- not publishing personal information
- not publishing information relating to the school community
- how to set appropriate privacy settings
- how to report issues or inappropriate content
- Un-moderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites

Social Media:
Chatrooms, blogs and other social networking sites are blocked by the schools filters so pupils do not have access to them in the school environment. However, we regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Internet Safety Education for pupils.

Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school's discipline policy and Safeguarding procedures.

Educational Use
School staff model appropriate use of school resources including the internet.
All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material.
Where appropriate, links to specific web sites will be provided instead of open searching for information.
In line with our e-safety curriculum, students will be taught how to conduct safe searches of the internet and this information will be made available to parents and carers.
Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Polices before any activity.
Staff and students will be expected to reference all third party resources that are used

How will pupils learn to evaluate Internet content?

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the SLT. 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 critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

How will parents' support be enlisted?

Parents' attention will be drawn to the School Internet Policy in newsletters, the school prospectus and on the school Web site.
Information on Internet use will be handled sensitively to inform parents without undue alarm.
A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

E-safety training

The school have a program of continuing professional development in place that includes whole school inset, in school support, consultancy and course attendance.
There is an induction process and mentor scheme available for new members of staff.
Educational resources are reviewed by all class teachers via the SMT and disseminated through curriculum meetings / staff meetings / training sessions

An e-Safety curriculum is in place and e-safety is embedded throughout the school curriculum and visited by each year group. Pupils are taught how to validate the accuracy of information found on the internet.

Data Security / Data Protection (see school data protection policy)

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998 .Data is stored on the school systems and transferred in accordance with the Becta Data Security Guidelines

Maintaining the security of the school ICT network:

We are aware that connection to the internet significantly increases the risk that a computer or computer network may be infected by a virus or accessed by unauthorised persons.

The school has ensured that **all** networked computers receive regular up-dates of Security virus protection. The school will make available to staff regular up-dates of Security virus protection for upgrading laptops and stand alone pc's, as updates are made available to school.
No Laptop should be connected to the school network without current and adequate virus protection.

Health and Safety:

St Joseph's have attempted, so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and in the ICT suite, which has been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards and Digital Projectors are being used.

Wider Community

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and password that will be recorded in the school office

Equal Opportunities - please refer to the schools Equal Opportunities and diversity policy.

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Safeguarding Policy.
Any suspected illegal activity will be reported directly to the police. The IT Team / Link2ICT Service Desk will also be informed to ensure that the Local Authority can provide appropriate support for the school.
Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Principal.
Breaches of this policy by staff will be investigated by the Principal. Action will be taken under Birmingham City Council's/MAC Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct.
All monitoring of staff use will be carried out by at least 2 senior members of staff.
Pupil policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the DSL and action taken inline with school anti-bullying and Safeguarding Policy.
There may be occasions when the police must be involved.

Serious breaches of this policy by pupils will be treated as any other serious breach of conduct in line with school Behaviour Policy.
Referral to Principal who may delegate to the SLT to investigate if appropriate.
For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
Minor pupil offenses, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school behaviour policy.
The Educations and Inspections Act 2006 grants the Principal the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.

How will complaints regarding Internet use be handled?

Responsibility for handling incidents will be delegated to a senior member of staff. (The e-safety co-ordinator at St Joseph's is Miss Olivia Harris) Any complaint about staff/ other adults misuse must be referred to the Principal. Pupils and parents will be informed of the complaints procedure. Parents and pupils will need to work in partnership with staff to resolve issues. Sanctions available include:

- interview/counselling by class teacher;
- informing parents or carers;
- removal of Internet or computer access for a period.

Depending on the seriousness of the incident – further more serious consequences may follow.

Appendices

A: School letter re "Responsible Internet Use - for Display"

St Joseph’s Catholic Primary School

Appropriate Use of Computers/Internet Use

We use the school computers and Internet connection for learning.

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

- I will ask permission before using the Internet.
- I will use only my own network login and password, which is secret.
- I will only look at or delete my own files.
- I understand that I must not bring software / USB memory sticks or discs into school without permission.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat.
- If see anything I am unhappy with or if I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right by electronic means to monitor the use of the school’s computer systems, including the monitoring of web-sites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school’s computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Display this page as a poster near computers.