St. Monica's Catholic Primary School Enfield

E-Safety Policy

Mission

Strive to succeed in the presence of God

Together as a Catholic Community,
Everyone Children, parents, staff and Parish
Achieves in their own unique way and strives to be
More like Jesus

CONTENTS

School e-Safety Policy

St Monica's Primary School's main Child Protection Officer will also act as the E-Safety Coordinator as the roles overlap. This is the Head teacher, Mrs Kate Baptiste.

Our e-Safety Policy has been written by the school. It has been agreed by the senior management team and approved by governors in April 2014.

The e-Safety Policy will be reviewed regularly by the Governing Body

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 functions.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access as it is an essential part of education in this current world.

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:
- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils world-wide;
- 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 across support services and professional associations;
- improved access to technical support including remote management of
- networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DfE;
- access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be 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.
- Staff should guide pupils in on-line activities that will support 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, retrieval and evaluation.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Use of Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Where practicable, access in school to external personal e-mail accounts, including webmail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

- Where feasible the school will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the Local Authority, LGFL and our Internet Service Provider to ensure filtering systems are up to date, regularly reviewed and as effective as possible.

Video Conferencing

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

Emerging Technologies

- Emerging technologies will be examined for educational benefit and potential risks before use in school is allowed.
- Mobile phones will not be used by the pupils for personal use during school time. Any children who bring a mobile phone to school, must turn it off and hand it in to the school office at the start and collect at the end of the day

School Web Site and Published Content

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Images that include pupils will be selected carefully and they will not be identified by name.
- Written permission from parents/carers is obtained before images of pupils are published electronically. This is done upon entry to school. Parents may subsequently write to agree/withdraw permission if they change their mind.
- Pupil's work can only be published with the permission of the pupil and parents.

Personal Data Protection& Security of Systems

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Security of the school ICT systems will be reviewed regularly.
- Virus protection is updated/reviewed on a regular basis.

E-Safety Complaints

- 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.
- Parents wishing to complain about an e-safety issue should use the established school complaints procedure.
- Complaints of a child protection nature must be dealt with in accordance with child protection procedures.

Communication of Policy

Pupils
- Rules for Responsible Internet Use are displayed in each classroom.
- Pupils will be made aware that Internet use will be monitored.

Staff
- All staff will be given access to the School e-Safety Policy and its importance explained.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents
- Parents' attention will be drawn to the School's e-Safety Policy in the school prospectus and the school website.

ST. MONICA'S CATHOLIC SCHOOL

E-Safety

Responsible Use of the Internet

Dear Parents

As part of pupils' curriculum enhancement and the development of ICT skills,
St. Monica's Catholic Primary School is providing supervised access to the Internet including e-mail.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet access provider operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavor is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, we are advised that the Governors cannot be held responsible for the nature or content of materials accessed through the Internet. The Governors will not be liable under any circumstances for any damages arising from your child's use of the Internet facilities.

I enclose a copy of the Rules for Responsible Internet Use that we operate at
St. Monica's.

Should you wish to discuss any aspect of Internet use please telephone me to arrange an appointment.

We ask parents of all children admitted to St. Monica's to sign the agreement.

Yours sincerely

K E Baptiste
………………………………………………………………………………………………

Permission for Internet Access

Parent/carer's permission
I give permission for my child to access the Internet as set out in the above letter.

Pupil's Agreement
I agree to follow the Rules for Responsible Use of the Internet (parent can sign on behalf of child as appropriate).

Signed: ……………………………………

Signed:………………………………

Print Name: …………………………………

Print Name:…………………………….

Date: …………………………………………..

Date:….………………………………

ST. MONICA'S CATHOLIC SCHOOL

Photograph Letter

July 20XX

Dear Parents

From time to time, photographs will be taken of your child for school purposes. This could be for a School Display, a record of School Performances or for the School's Website. (If photographs are put onto the website, children are never identified by name.)Parents have the right to request that their child is not included in photographs for school use.

If you have no problem in allowing your child either now or in the future having their picture taken, then please give your consent by signing below.

However, if you do object to this in either the short or long-term future of your child's life here at St. Monica's School then please send in a separate letter to me addressed "PHOTOGRAPH LETTER".

Yours sincerely

K E Baptiste

PHOTOGRAPH PERMISSION LETTER

Name of child: ………………………………………… Class: …………

I give permission for my child to have their photograph taken as and when the occasion arises and for it to be displayed

Signed: ………………………………………… (print name) ………………...

Date: ………………………………………………………………………………

St Monica's Catholic Primary School

E-Safety

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 ask permission from a member of staff before using the Internet;

- 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 school work and homework;

- I will not bring USB memory sticks into school unless I have permission;

- 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 give my home address or phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;

- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;

- I understand that the school may check my computer files and may monitor the Internet sites I visit.

St Monica's Catholic Primary School

E-Safety

Staff ICT/E Safety Acceptable Use Agreement

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password.

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted.

- I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.

- I have read and understood the school e-Safety policy

- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator (Kate Baptiste) and/or the e-Safety Coordinator (name) as soon as possible, (or in her absence, Mike Ross).

- I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (Kate Baptiste) the e-Safety Coordinator.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team (Breda Ryan) as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school policy and the Law.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Council, into disrepute.

- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator (Kate Baptiste)

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

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Agreement.

My Name

Signed   Date