E-safety policy at Birchley St. Mary's

Created December 2009
Reviewed July 2014

Mission Statement

Birchley St. Mary's Catholic Primary School

* * * * *

**St. Mary's School
is a safe and happy place,
where we follow Jesus by
living, loving, learning
and working together.**

Our school family aims to understand and follow the example set by Jesus.

We will achieve this by:

- Using the Archdiocesan syllabus to underpin all school policies and practices.
- Developing self respect and respect of others.
- Setting good examples of positive behaviour.
- Encouraging and rewarding honesty and integrity.
- Listening to each other.
- Enabling all to contribute.
- Enabling all to recognise their actions and resulting consequences.
- Providing quality opportunities for silent prayer and/or reflection.
- Facilitating opportunities for helping others.

Our school family aims to fully develop the potential of everyone within our school community.

We will achieve this by:

- Providing a broad, balanced and creative curriculum, accessible by all.
- Having rigorous and robust assessment procedures which drive teaching and learning.
- Seeking enrichment opportunities.
- Celebrating success and achievement at every level.

Our school family aims to work together with our families and parish to be an integral part of the wider community.

We will achieve this by:

- Actively seeking out opportunities to promote the school as part of the wider community.
- Actively seeking out opportunities to enrich the local and wider community
- By encouraging links with the parish and families
- Involving local community in school/parish events.
- Making effective use of visitors to enhance the children's learning.
- Developing means of communication e.g. newsletters, reports, parent evenings and websites.

Our e-safety policy has been written by the school, building on the Kent NGfL policy, Bracknell Forest, LA ICT Advisory Group recommendations and government guidance. It has been agreed by the senior management, approved by governors and shared with our School Council. It will be reviewed annually.

Created by: Kelly Waring

Date: December 2009

To be revised: July 2015

Approved: January 2010

Why is internet use important?
- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The internet is an essential element in 21st century 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.

How does the internet benefit education?

Benefits of using the internet in education include:
- Access to world-wide educational resources;
- Educational and cultural exchanges between pupils world-wide;
- 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;
- Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LA and DfES.
- Mentoring of pupils and provide peer support for them and teachers.

How will internet use enhance learning?

- The school internet includes a filtering service appropriate to the age of pupils.
- Pupils will continually be taught about acceptable use of the internet and continually 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 guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, evaluation and retrieval.

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 ICT co-ordinator.
- Children minimise or turn off the screen if they see any images that they are not comfortable with. They will report site to the teacher, who will make ICT co-ordinator aware, this will get reported to the LA immediately. Parents will also be informed.
- School will provide opportunities to discuss copyright with pupils and staff ensure that internet derived materials comply with copyright law.

How will e-mail be managed ensuring safety for pupils?

- 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 via a personal web space, such as address or telephone number, or arrange to meet anyone.
- Personal email or messaging between staff, parents and pupils should not take place, including the use of social network sites like facebook.
- Whole-class or group e-mail addresses should be used at Key Stage 1 and below.
- E-mail sent to an external organisation 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.
- Emails (internal and external) are archived for six years and strictly monitored by the LA.
- Year 6 have a scheme of work for the appropriate use of emails.
- We hold an annual 'Internet Safety Week' where all staff and children take part in activities to promote safe use of the internet,

How should website content be managed?
- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- The office manager, in consultation with the senior leadership team, will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce it has been obtained.

Chat and instant messaging

- Pupils will not be allowed access to public or unregulated chat rooms.
- Pupils will not access social networking sites, for example, 'My Space' or 'Bebo'.
- Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.
- Any form of bullying or harassment is strictly forbidden.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.
- Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant

messaging or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first and appropriate professional language should always be used.

-

Personal websites and blogs

- Pupils will not access social networking sites for example 'My Space' or 'Bebo'.

- When publishing material to websites and elsewhere, pupils should consider the thoughts and feelings of those who might view the material. Material that victimises or bullies someone else, or is otherwise offensive, is unacceptable.

Photographic, video and audio technology

- When not in use, video conferencing cameras should be switched off and turned to face a wall.
- It is not appropriate to use photographic or video devices in changing rooms or toilets.
- Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.
- Staff may use digital cameras or video devices to support school trips and curriculum activities.
- Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken.
- Pupils should always seek the permission of their teacher before making audio or video recordings within school.

How can emerging ICT applications be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time.
- The sending of abusive or inappropriate text messages is forbidden.
- Pupils should not bring mobile phones into school.
- Mobile phone cameras should not be used.

How will internet access be authorised?

- The school will keep a record of all pupils who are granted internet access. The record will be kept up-to-date and each teacher will be aware of children who do not have permission for their pictures to be published on the internet.
- At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised internet access.
- Parents will be asked to sign and return a consent form.
- Children and staff will sign a consent form to agree to rules and regulations of internet use

How will the risks be assessed?

- In common with other media such as magazines and books, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. We will use a filtering system monitored by the LA to prevent access to unsuitable sites. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor St. Helens Council can accept liability for the material accessed, or any consequences of internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher will ensure that the e-Safety policy is implemented and compliance with the policy monitored.
- Access is strictly forbidden to any websites that involve gambling, games or financial scams.

How will filtering be managed?

- The school will work in partnership with parents, the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.
- Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.org.uk).
- We use a filtering system monitored by the LA to prevent access to unsuitable sites.

How will the pupils be made aware of this policy?

- Rules for internet use will be posted in all rooms where computers are used.
- Pupils will be informed that internet use will be monitored.
- Instruction in responsible and safe use should precede internet access.
- A module on internet safety is covered throughout the school.
- Staff will be role models for the safe use of the internet and constantly remind children of rules when using the internet.
- Parents will receive information on how to keep children safe on the internet at home and therefore support our school policy and rules.
- We begin each year with discrete teaching of e-safety, as well teaching in line with National e-safety day in February. E-safety underpins everything that we do.

How will staff implement this policy?

- All staff and students must accept the terms of the 'Responsible Internet Use' statement before using any internet resource in school. This includes supply and non-teaching staff.
- All new staff will be taken through the key parts of this policy as part of their induction.
- All new staff will be provided with a copy of this policy.

- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School e-Safety Policy and have its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in safe and responsible internet use and on the school internet policy will be provided as required.
- Breaching this e-safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.
- Emails will be monitored. Enterprise Vault archives items from your mailbox. Enterprise Vault archives all types of information stored in private computer, including messages, documents, spreadsheets, graphics, and voicemail.
- Use of portable media such as floppy disks, memory sticks and CD-ROMs are only to be used when necessary. Confidential information and children's full names and personal information should never be kept on such devices.
- Portable media may not be brought into school without specific permission and a virus check.
- Files held on the school's network will be regularly checked.

How will complaints regarding internet use be handled?

- Responsibility for handling incidents will be delegated to the ICT co-ordinator who may refer the incident to a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues. Children may be stopped from using the internet or

computer for a period, which could ultimately prevent access to files held on the system.

- There may be occasions when the police must be contacted immediately.
- Complaints of a safeguarding nature must be dealt with in accordance with LA/BFBC safeguarding procedures – see flow chart.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School e-safety Policy in newsletters.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. Suggestions for safe internet use at home will be provided.
- Workshops will be held for parents to be made aware of how to support safe use of the internet at home
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.
- Parents will be made aware of websites to support internet safety, such as, CEOP and Think U Know.

Response to an Incident of Concern

The screening tool is available on the Children's Safeguards Service website.

A concern is raised

Refer to school's designated child protection co-ordinator

What type of activity is involved? (Use screening tool)

Illegal

Neither → Incident closed (is counselling or advice required?)

Inappropriate

Who is involved?

Child as instigator — Establish level of concern. (Screening tool)

Child as victim — Establish level of concern. (Screening tool)

Staff as victim — Establish level of concern. (Screening tool)

Staff as instigator — Establish level of concern. (Screening tool)

Potential illegal or child protection issues?

No

Yes

Other children involved?

Yes

No

Refer to Children's Safeguards Service

If appropriate, disconnect computer, seal and store.

In-school action: designated CP co-ordinator, head of ICT, senior manager.

Counselling Risk assessment

Manage allegation procedures

Possible legal action

School disciplinary and child protection procedures. (possible parental involvement)

Possible legal action