All Souls' Catholic Primary School

INTERNET SAFETY AND ACCEPTABLE USE POLICY

December 2012

All Souls' Catholic Primary School

Internet Safety and Acceptable Use Policy

Rationale

The Internet is becoming as commonplace as the telephone or television and its effective use is an essential skill in everyday life. In preparing children for the adult world ahead, schools have a duty to embrace new technology and harness the potential learning experiences that it offers. Unmediated Internet access, however, does bring with it the possibility of placing pupils in embarrassing, inappropriate, incriminating and even dangerous situations. Therefore, it is crucial that strategies are in place to safeguard all users of the Internet within schools as well as to protect the ICT infrastructure from potential harm.

Aims

- To provide a clear framework for the acceptable use of computers and the Internet within school.
- To support the ICT curriculum policy in ensuring that technology is widely available and used to enhance the curriculum and provide learning opportunities that without Internet use, would be impossible.
- To protect all members of the school from potential harm resulting from misuse of technology.
- To instil confidence in teachers to deliver ICT enriched lessons.
- To provide clear guidance on procedure in the instance of misuse.
- To ensure that online safety remains a high priority within the curriculum and that children learn to become 'responsible' Internet users.
- To make explicit the roles and responsibilities of all adults within school with regards to safe use of technology.

Implementation

<u>Pupils' use of the Internet as part of the curriculum</u>

Within all aspects of the curriculum, the Internet has much to offer pupils and an important role to play. Teachers are expected to ensure that 'new technologies', including the Internet, are used effectively to enhance teaching and learning and so pupils will have regular access to the Internet within lessons in many different contexts:

- Visiting specific websites selected by the teacher
- Using search engines to research topics
- Using information provided by the teacher, sourced from the Internet
- Multimedia content – i.e. video clips, sounds and images

Whilst through the local authority firewall and filtering service, the vast majority of potentially offensive content is blocked, it is impossible to guarantee that no inappropriate material could be accessed. To minimise the possibility of pupils accessing such content, teachers should, where possible stringently vet all websites which they are asking pupils to view.

Before pupils are given access to the Internet, teachers should make them aware that they may come across inappropriate content and that if they do, they should inform a school adult immediately or if they felt too embarrassed, their parents. Parents should be made aware that if their child discloses that they were exposed to inappropriate material at school, and haven't spoken to a member of staff, then they should notify the school of this incident. Equally, if an incident is reported to a member of staff, then the parents of that child should be notified by school. All incidents of inappropriate content will be recorded on the school's electronic recording system.

Increasingly, children may use email as part of the curriculum, particularly in KS2. In these instances, pupils will use only the email accounts issued to them by the school and will only be allowed to use these accounts within directed teaching sessions at school. Children should be aware that they may receive SPAM or emails from people that they do not recognise. Again, these instances should be reported and recorded as described above. In addition, to ensure that children themselves are using email appropriately, the network manager should routinely undertake random monitoring of email accounts and report to the Headteacher.

Pupils have no access within school to newsgroups or social media sites. Through Internet Safety education we remind children that the vast majority of social media sites operate a policy of only allowing persons over the age of 13 to register, and that registering outside of these terms and conditions is illegal. However, through the school's e-safety and cyber bullying programme we will educate children as to the safe usage and benefits of social media sites and as well as the dangers presented. Although the event of cyber bulling taking place in school is incredibly unlikely, incidents which occur outside of school are more common place. Whilst as a school we are not obliged to deal with incidents occurring outside of the school day and premises, we will always support parents in resolving any issues which we feel may impact children inside of school.

Children should be not be allowed access to chat rooms for any purpose during the school day. Again the relative merits and dangers associated with their use will be discussed with the children as part of the school's e-safety programme.

All pupils with KS1 and KS2 are issued with a memory stick which remains in a locked cabinet in each classroom. These memory sticks are to be used under the supervision of the class teacher and only for the purpose of in school curriculum activities. Under no circumstances should the school memory stick be taken home on off site. Equally, memory sticks brought in from home for the purpose of homework etc. should undergo a strict virus and content scan by the network administrator or a trained member of staff before being used or accessed. Children should be encouraged to email work to school as opposed to bringing it in using removable media.

Children should be educated as to what 'piracy' means and its impact on the wider world.

Staff use of the Internet

Staff have access to the same Internet steam as pupils and therefore within the filtering system. Staff should adopt the rule that they should only use the school's Internet facility to support them in successfully fulfilling their role within school. This will include the use of the school email system.

Staff should not make use of personal email, social media sites (e.g. Facebook, twitter etc) or online sites such as eBay and online stores through the school's internet stream, or via their personal mobile devices during directed working hours.

In the instance of staff receiving inappropriate or offensive emails through their school email account, these should be reported to a member of the senior leadership team at the earliest convenience.

Staff also need to be made aware that their behaviour and use of the Internet outside of school needs to fall within the requirements as set out in the teacher standards irrespective of their role or position in school. Under no circumstances should staff make any reference, no matter how insignificant, to any school related business, on the Internet which does not relate to their role or responsibilities within school.

Although not an exhaustive list, staff should adhere to the following specific guidelines:

- Do not, under any circumstances, accept friend requests from a person you believe to be either a parent or a pupil at your school.
- Do not use Internet or web-based communication channels to send personal messages to a child or parent.
- Bear in mind that someone else could post a photo on their profile in which you are named, so think about any photos in which you appear. If you do find inappropriate references to you and/or images of you posted by a 'friend' online, you should contact them and the site to have the material removed so as to protect yourself.
- Be aware that anybody may have access to your profile. Therefore you must mind your language and behaviour such as not to cause offense or lead to complaints against you to your employer.
- Ensure that any comments and or images could not be deemed as defamatory or in breach of copyright legislation or illegal.
- Always make sure that you log out of social media sites after using them.

Teaching staff are issued with a school memory stick, which should be used for school purposes only. These memory sticks should only be used on school computers, laptops or machines in trusted locations e.g. other schools, Elm Bank etc. Preferably, personal memory sticks should not be used. However, staff wishing to use them, or portable hard driver or other removable media, should ensure that they have undergone the rigorous virus checks as per children's memory sticks.

Staff should also be aware that it is their responsibility to ensure that all of the materials and media that they use, including those sourced on the Internet, are not in breach of copyright legislation.

All staff should be made aware that any personal information or records which they come into contact with at school are strictly confidential and should under no circumstances be disclosed to anyone inside or outside of school without the headteacher's permission.

In the event of any school information or data being lost or stolen, a member of the SLT should be informed immediately.

Incidents of misuse

All incidents which are not in line with this policy are to be recorded using the school's electronic recording system and reported to governors. In the event of a member of staff disregarding the policy it would be considered as misconduct and would have to be investigated in accordance with the school's disciplinary procedures.

Internet safety education

Through both ICT and PSHE lessons, children are education in the safe use of technology. The teaching of safety should precede any use of technology within lessons. The school makes use of the resources produce by the CEOP and use the national 'Internet Safety Week' to further promote safe internet use. The SLT keep up to date with good practice guidance and legislation and ensure that teaching staff are updated through staff meetings and INSET.

Home/School Agreement

Through the Home/School agreement, children and parents subscribe to this policy and accept their roles and responsibilities in relation to Internet safety.

Monitoring and Review

It is the responsibility of the SLT to ensure that this policy is updated, adhered to and made widely available. It is the headteacher's responsibility to report on the effectiveness of the policy and any breaches of safety.

This policy should be reviewed annually or in the instance of legislative changes.

Chair of Governors: Shirley Langford	**Signed:**
Agreed at Governing Body Meeting:	**12 December 2012**
To be Reviewed:	**December 2013**