E-SAFETY POLICY

SACRED HEART RC NURSERY & PRIMARY SCHOOL

Persons responsible for this policy: Nichola Day / Diana Smith

Written: October 2015
Review Date: October 2016
Agreed by governors: November 2015

Introduction

The Internet is now regarded as an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones and touch screen tablet devices.

Computer skills are vital to access life-long learning and employment; indeed computing is now seen as an essential life-skill.

Young people have access to the Internet from many places, home, school, friendsôhomes, libraries and in many cases mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe. This policy is designed to ensure safe internet use by pupils in school, but also while on-line at home etc.

1. Core Principles of Internet Safety

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

2. Why is Internet use 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.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, well-being and to support the professional work of staff and to enhance the schoolôs management information and business administration systems.

3. How will Internet use enhance learning?

- The school Internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.
- Pupils will learn appropriate Internet use and be 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.

4. How will Internet access be authorised?

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance a member of staff may leave or a pupilôs access be withdrawn.
- Parents will be informed that pupils will be provided with supervised Internet access (an example letter for primary schools is included as an appendix).

5. How will filtering be managed?

- The school will work in partnership with parents and Lee Wade IT Services to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils discover unsuitable or illegal sites, the URL (address) and content must be reported to the ICT co-ordinator (Mrs Diana Smith). Parents of the children involved will be notified immediately.
- ICT Leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

6. How will the risks be assessed?

- In common with other media such as magazines, books and video, 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. 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 CAST 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, Designated Safeguarding Lead and ICT leader will ensure that the Internet policy is implemented and compliance with the policy monitored.

7. Managing Content

7.1 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 ICT Coordinator.
- Specific lessons will be included within the Computing Scheme of Work that teaches all pupils how to read for information from web resources.
- Nominated persons (ICT Coordinator) will be responsible for permitting and denying additional websites as requested by colleagues.

7.2 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 pupilsôhome information will not be published.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name.
- Pupilsôfull names will not be used anywhere on the website, particularly in association with photographs.
- Signed permission from parents or carers will be obtained before photographs of pupils are published on the school website

8. Communication

8.1 Managing e-mail

- Pupils may only use approved e-mail accounts on the school system, DB Primary.
- Pupils must immediately tell a teacher if they receive offensive e-mail or óblow the whistleôon DB Primary, alerting key member of staff.
- Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.

- 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.

8.2 On-line communications and social networking

- Safe use of Social Network sites will be taught as part of the computing curriculum. Support of the local PCSO will be sought with regards to Social Network sites.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Bi-annual V-Safe workshops for parents.
- Pupils will be advised to use nicknames and avatars when using social networking sites as part of the e-safety programme and to use all the available privacy settings.

8.3 Mobile technologies

- Appropriate use of mobile phones will be taught to pupils as part of their e-safety programme.
- Pupil mobile phones are not permitted to be in the childôs possession when in school. Phones are handed in to the school office at the start of the day and collected at the end.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

9. Introducing the Policy to Pupils

- Rules for Internet access will be posted in all rooms where computers are used.
- A module on responsible Internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.
- Instruction on responsible and safe use should precede Internet access.
- Pupils will be informed that Internet use will be monitored.

10. Parents and E-Safety

- Parentsôattention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school website.
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues 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.
- All parents will receive support information as and when available.

11. Consulting with Staff and their inclusion in the E-safety Policy

- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.

- The schoolôs consequences for Internet and mobile phone / PDA / technology misuse will be clear so that all teachers are confident to apply this should the situation arise.
- All staff must accept the terms of the óResponsible Internet Useô statement before using any Internet resource in school.
- Community users of the schoolôs ICT facilities must sign the acceptable user policy before being granted access.
- Staff development in safe and responsible Internet use and on the schoolôs Computing and ICT policy will be provided as required.

12. How will complaints be handled?

- Responsibility for handling incidents will be delegated 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.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Sacred Heart Nursery & Primary School

Pupil Acceptable Use Agreement/e-Safety Rules

Dear Parent/Carer
ICT including the internet, email, laptops, digital cameras etc are an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please discuss these eSafety rules with your child. If you have any concerns, please contact the school which holds an ICT policy and an e-Safety policy.

- I will only use ICT in school for school purposes.
- I will only use my DB Primary email address.
- I will make sure that all ICT contacts with other children and adults are responsible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will turn off my monitor and tell my teacher immediately.
- I will not send to children or adults anything that could be considered unpleasant or nasty.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.

e-Safety Agreement
Name of child
é é é é é é é é é é é é é é é é é .é é é é é é é é é é é é Classé é

We have discussed this and my child agrees to follow the e-Safety rules and to support the safe use of ICT at Sacred Heart Nursery & Primary School.

Parent/ Carer Signature

é .é é Dateé é é é é

Sacred Heart RC
Nursery & Primary School

Sample Letter to Parents

1 September 2015

Dear Parents/Carers

Responsible Internet Use

As part of your childôs curriculum and the development of their ICT skills, Sacred Heart Primary and Nursery School provides supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. All children begin the academic year learning about e-safety and follow the SMART rules to keep them safe when using the internet. These are displayed in the ICT suite to remind the children how to use the internet safely and responsibly. Please would you read the attached Acceptable Use agreement and sign and return the consent form so that your child may use the Internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider, Precedence, operates a filtering system that restricts access to inappropriate materials. Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your childôs use of the Internet facilities. Should you wish to discuss any aspect of Internet use please telephone the school to arrange an appointment with either your childôs class teacher, Mrs Day (Designated Safeguarding Lead) or Mrs Diana Smith (ICT Leader).

Yours sincerely

Mrs Nichola Day
Deputy Headteacher / Designated Safeguarding Lead

Staff Laptop Policy

Sacred Heart RC
Nursery & Primary School

1. The laptop remains the property of Sacred Heart School.
2. The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Sacred Heart Primary and Nursery School Staff should use the laptop.
3. On the teacher leaving the schoolŝ employment, the laptop is returned to Sacred Heart Primary and Nursery School.
4. Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the headteacher).
5. When in school and not being used, the laptop must be kept in an office or cupboard. It must not be left unattended classroom.
6. Where the laptop is taken out of school, it must not be left in an unattended car. If there is a need to do so it should be locked in the boot.
7. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.
8. Staff may load their own software onto the laptop but it must be fully licensed and not corrupt any software or systems already installed on the laptop.
9. Any software loaded must not affect the integrity of the school network.
10. If any removable media is used then it must be checked to ensure it is free from any viruses.
11. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
12. If any fault occurs with the laptop, it should be referred to Gareth Jones or Lee Wade IT Services.
13. The laptop would be covered by normal household insurance. If not it should be kept in school and locked up overnight.

Signed:

Date:

Sacred Heart RC
Nursery & Primary School

Policy for Responsible e-mail, Network and Internet Use

1. I will use all ICT equipment issued to me in an appropriate way. I will not:

- Access offensive website or download offensive material.
- Make excessive personal use of the Internet or e-mail.
- Copy information from the Internet that is copyright or without the ownerôs permission.
- Place inappropriate material onto the Internet.
- Will not send e-mails that are offensive or otherwise inappropriate.
- Disregarded my responsibilities for security and confidentiality.
- Download files that will adversely affect the security of the laptop and school network.
- Access the files of others or attempt to alter the computer settings.
- Update web pages etc. or use pictures or text that can identify the school, without the permission of the headteacher.
- Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Sacred Heart Primary and Nursery School.

2. I will only access the system with my own name and registered password, which I will keep secret.

3. I will inform the ICT Schoolôs Technician, Gareth Jones, as soon as possible if I know my password is no longer secret.

4. I will always log off the system when I have finished working. ·

5. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.

6. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the headteacher and register the passwords with the headteacher.

7. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.

8. I will not open e-mail attachments unless they come from a recognised and reputable source.

9. I will bring any other attachments to the attention of the ICT technician.

10. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.

11. I will report immediately to the headteacher any unpleasant material or messages sent to me.
12. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.

13. Use for personal financial gain, gambling, political purposes or advertising is forbidden.

14. Storage of e-mails and attachments should be kept to a minimum to avoid unnecessary drain on memory and capacity.

15. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.

I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

Name..
Signature: ....
Date: ....

13. Web-based Resources

www.thinkuknow.co.uk/parents

www.childnet.com/resources/know-it-all-for-parents

www.saferinternet.org.uk/advice-and-resources/parents-and-carers

www.kidsmart.org.uk/parents

www.e2bn.org/esafety/224/e-safety-for-parents-sessions

Report abuse here
http://ceop.police.uk/