The Catholic Primary Schools of The Waveney Valley

ST BENET'S AND ST EDMUND'S

FEDERATION OF CATHOLIC PRIMARY SCHOOLS

e-Safety Policy

DATE: 09.07.14

CHAIR OF GOVERNORS: - David Lowe_____

DATE OF REVIEW: - July 2016

The Catholic Primary Schools of The Waveney Valley

Introduction

The schools e-Safety Policy covers the safe use of internet and electronic communications technologies. The internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT.

The policy highlights the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It also provides safeguards and rules to guide staff, pupils and visitors in their online experiences.

Computer skills are vital to access life-long learning and employment. Our School has 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. We provide pupils with as safe an internet environment as possible, and teach them to be aware of, and respond responsibly to possible risks.

The schools e-safety policy operates in conjunction with others, e.g. Behaviour, Anti- Bullying, Acceptable Use, Teaching and Learning, Data Protection, and Safeguarding Children.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A clear understanding of the e-Safety Policy;
- Secure, filtered broadband from Suffolk County Council (E2BN);
- A school network that complies with the National Education Network standards and specifications.

Core Principles of Internet Safety

Guided educational use

Significant educational benefits result from curriculum internet use including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum internet use should be planned within a regulated and managed environment. Directed and successful internet use will also reduce the opportunities for activities of dubious worth.

Risk assessment

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become „internet wise". Our school is fully aware of the risks, perform risk assessments and implement a policy for internet use. Pupils know how to respond if they come across inappropriate material.

Responsibility

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. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. For instance, un-moderated chat rooms present immediate dangers and are banned. Fair rules prominently displayed at the point of access help pupils make responsible decisions.

Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies are selected to suit the school situation and their effectiveness monitored.

- There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

Teaching and learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to our primary age pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are taught in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

Managing Internet Access

Information system security

- The School's ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail –Key Stage 2

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- **Photographs that include pupils will be selected carefully where permission has been gained. In the main, group photographs will be used rather than full-face photos of individual children.**
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- **Written permission from parents or carers will be obtained at the beginning of their child's education before photographs and/or work of pupils are published on the school Web site.**
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing

- Pupils will **not** access social networking sites within school, but will be educated in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- 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.

Managing filtering

- The schools" broadband provider is E2BN, who is recommended by SCC.
- **If staff or pupils come across unsuitable on-line materials, the site must be recorded in a folder kept in the staffroom** and will be reported to the e-Safety Coordinator who will take the relevant steps to ensure that filtering methods selected are effective.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team are aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones (staff) will not be used during school time (8:35am-12:00, 1:00-3:15). If staff use these they need to do this away from other staff and children.
- Staff may be issued with a school phone for off site educational visits.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

- All staff must read the Acceptable Use Policy before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources form before being allowed to access the internet from the school site.
- Key Stage 2 have access to the Internet for independent research which is supervised by an adult.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor SCC can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is appropriate and effective.

Handling 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 headteacher.
- Complaints of a safeguarding nature will be dealt with in accordance with school safeguarding procedures. (Our School" s e-Safety Policy has a flowchart of responses to an incident of concern.)
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy

Introducing the e-safety policy to pupils

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed (with reference to the materials from SCC).
- e-Safety training will be embedded across the curriculum.

Staff and the e-Safety policy

- All staff will be referred to the School e-Safety Policy and its importance explained.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

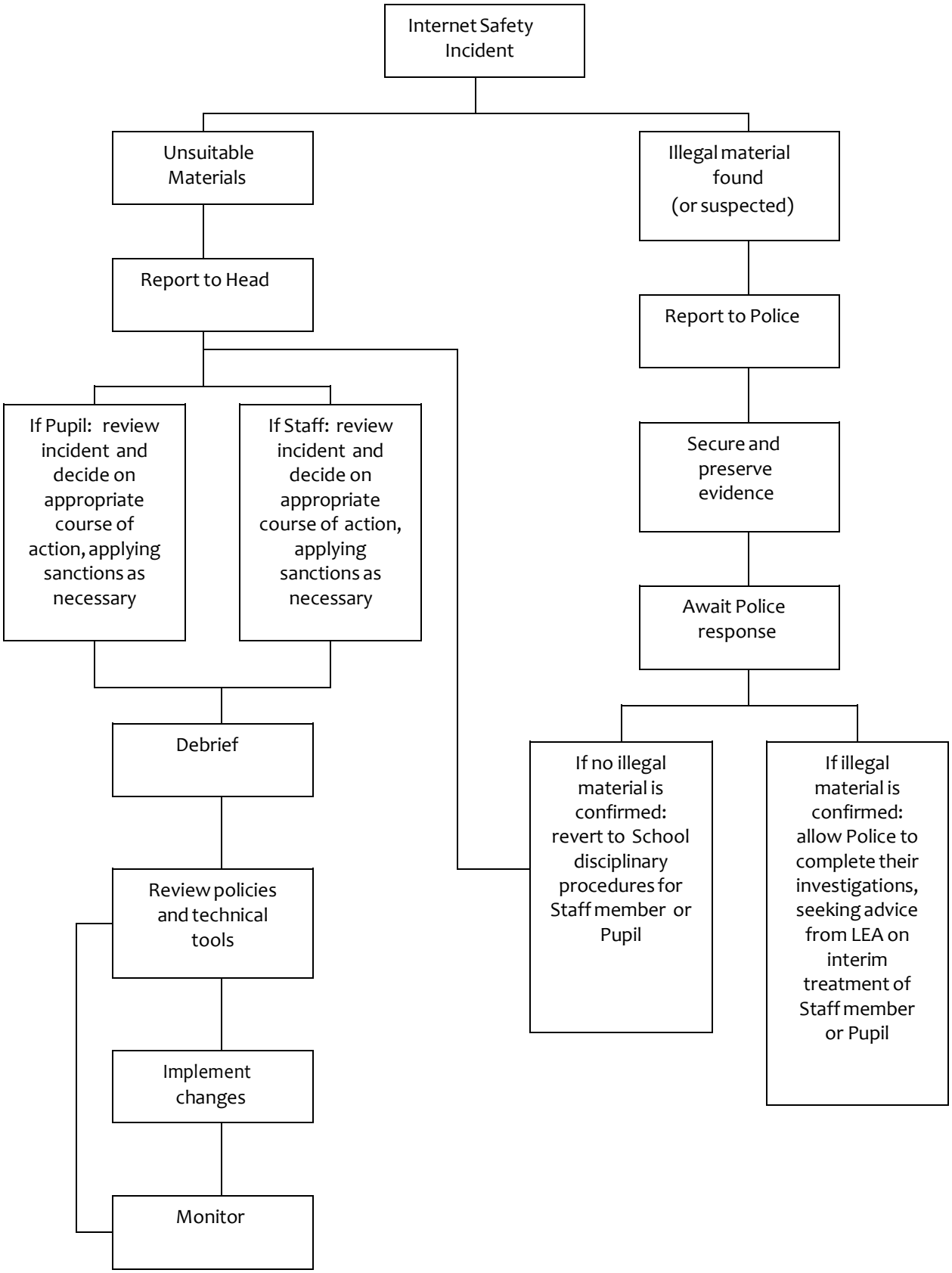
Parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Any Parent / Carer wishing to access the internet via the Family Information Point must sign in the acceptable use of School ICT Resources file.

Appendix 1 : Internet use

Possible teaching and learning activities Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e- mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	RM EasyMail SuperClubs Plus School Net Global Kids Safe Mail
Publishing pupils" work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils" full names and other personal information should be omitted. Pupils" work should only be published on „moderated sites" and by the school administrator.	Making the News SuperClubs Plus Headline History National Education Network Gallery
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art National Education Network Gallery
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Plus FlashMeeting
Audio and video conferencing to gather information and share pupils" work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives "On-Line" Global Leap JANET Videoconferencing Advisory Service (JVCS)

Appendix 2 : Internet Safety Incident Flowchart



Appendix 3 : Safe Rules for Responsible Internet Use

See displayed posters

(Example of wording)

Key Stage 2

- ✓ I will ask permission before using the Internet.
- ✓ If I see anything I am unhappy with on the Internet I will turn off/close the screen and tell an adult immediately.
- ✓ I will only e-mail people that my teacher has approved.
- ✓ I will only send e-mails that are polite and friendly. I will never open e-mails sent by anyone I don't know.
- ✓ I will never give out a home address, phone number or arrange to meet someone. I will ask permission each time I need to connect a pen-drive to the computer.
- ✓ I will not access other peoples' files. I will never use Internet chat rooms.

Foundation/ Key Stage 1

- ✓ I will only use the Internet when an adult is present.
- ✓ I can only click on the buttons or links when I know what they do.
- ✓ I can search the Internet when an adult is present.
- ✓ I always ask if I get lost on the Internet

Headteacher : Mr Ivan Mulinder

DATE…

Internet Use - Parent / Carer Permission

As part of the school's Information and Communication Technology (ICT) programme we offer the children supervised access to the Internet. This will allow children to explore thousands of libraries, databases and as they move through the school, to exchange messages with other school Internet users.

The benefits are enormous and support and enhance all areas of the curriculum. The Suffolk Computer system has a filter, which prevents children accessing any information that is inappropriate. We will supervise and ensure that the children only access information appropriate to their age group and in line with our schemes of work and school policy. Clear guidelines and safety rules are explained to the children.

We must obtain parental permission before allowing Internet access and therefore ask you to sign the attached form and return it to school. This letter will be sent out yearly as the rules will progress through each key stage.

Yours sincerely

HEADTEACHER
Mr Ivan Mulinder

Parent / Carer Permission

I have explained the Safe Rules for Responsible Internet Use to my child. We both understand the rules for Responsible Internet Use.
I give permission for …….. to access the Internet at Pakefield Primary School under teacher supervision.

Signed ……Name

……. Date

…… Class……..

.

The Catholic Primary Schools of The Waveney Valley

Appendix 5 : Useful resources for Parents / Carers

Care for the family www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD http://publications.teachernet.gov.uk

Family Online Safe Institute www.fosi.org

Internet Watch Foundation www.iwf.org.uk

Parents Centre www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com

Appendix 6 : Useful resources for teachers

BBC Chat Guide Video + "What If…" Discussion Cards
(Available from the „Teachers Documents Folder on the School's Intranet)

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Becta http://schools.becta.org.uk/index.php?section=is

Chat Danger
www.chatdanger.com

Child Exploitation and Online Protection Centre www.ceop.gov.uk

Childnet www.childnet-int.org

Cyber Café http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org

Kidsmart
www.kidsmart.org.uk

Think U Know
www.thinkuknow.co.uk

Safer Children in the Digital World
www.dfes.gov.uk/byronreview

Appendix 7:

Acceptable Use of Family Information Point

- I will only access the computer and Internet as instructed
- I will not try to access any other files or areas of the network
- I will not download program files from the Internet
- Any Emails or messages that I send will be polite and sensible
- To help protect myself and others, I will tell a member of staff 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 my computer usage including any Internet sites that I visit.

Agreement

I have read and I understand the rules for Responsible Internet Use, and will sign and date my use in the Family Information Point file.

Appendix 8 : e-Safety Audit

Has the school an e-Safety Policy that complies with SCC guidance?	**Y/N**
Date of latest update:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff at:	Y/N
The policy is available for parents/carers at:	School website
The responsible member of the Senior Leadership Team is:	Mrs G Taylor
The responsible member of the Governing Body is:	CHAIR HSW
The Designated Safeguarding Manager is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both pupils and staff?	**Y/N**
Is there a clear procedure for a response to an incident of concern?	**Y/N**
Are SCC approved e-Safety materials available to employees?	**Y/N**
Are employees given the Acceptable Use Policy during induction?	**Y/N**
Are all pupils aware of the School" s e-Safety Rules?	**Y/N**
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	**Y/N**
Do parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules?	**Y/N**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y/N**
Has an ICT security audit been initiated by SLT, possibly using external expertise?	**Y/N**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y/N**
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g. SCC)?	**Y/N**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y/N**