St Louis Catholic Academy

‘Loving to Learn – Learning to Love’

e-Safety Policy 2016-2017

Purpose: To give clear, unambiguous guidance to pupils, parents and staff in order to minimise any risks to our children through increased Internet usage and to ensure good practice throughout the school which is understood by pupils, parents/carers and staff.

Date: 2 February 2016

Introduction

1. Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT & Computing, bullying and for child protection.

- The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on Kent County Council's e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors and the Friends Association.
- The e-Safety Policy and its implementation will be reviewed annually.

2 Teaching and learning

2.1 Why Internet use is 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Internet & VLE use will enhance learning

- The school Internet and VLE access will be designed expressly for pupil use and will include 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.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

2.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3 Managing Internet Access

3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Suffolk LEA.

3.2 E-mail & VLE

- Pupils may only use approved e-mail and VLE 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.
- 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.

3.3 Published content and the school web site

- 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 Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4 Publishing pupil's images and work

- 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 Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.

3.5 Social networking and personal publishing

- The school will block/filter access to social networking sites.
- 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 or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

3.6 Managing filtering

- The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7 Managing videoconferencing

- 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.

3.8 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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

3.9 Protecting personal data

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

4 Policy Decisions

4.1 Authorising Internet access

- All staff must read the VLE pupil agreement and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- 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 pupil's access be withdrawn.
- 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 asked to sign and return a consent form.

4.2 Assessing risks

- 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 Suffolk County Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

4.3 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 child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

- Pupils have the facility to ‘blow the whistle’ on DB Primary VLE to alert adults in a safe and confidential manner.

4.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

5 Communications Policy

5.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each term.
- Pupils will be informed that network and Internet use will be monitored.

5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and 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.

5.3 Enlisting parents’ support

- Parents’ attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

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 Kent Grid for Learning (Tunbridge Wells Network)
Using search engines to access information from a range of websites.	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.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	RM EasyMail SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites. VLE (password protected)	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History Kent Grid for Learning Focus on Film
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.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
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 Skype FlashMeeting
Audio and video conferencing to gather information and share	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail	Skype FlashMeeting National Archives "On-

pupils' work.	address or protected password should be used.	Line" Global Leap National History Museum Imperial War Museum

Staff, Governor and Visitor

ICT - Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr. Grey**,** St. Louis Catholic Primary school e-Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of the ICT coordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature …….………………….………… Date ……………………

Full Name ………………………………….................................... *(Printed)*

Job title . . . .

Primary Pupil Acceptable Use
Agreement / e-Safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my class email address or my own school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ 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 tell my teacher immediately.
- ✓ 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 will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- ✓ 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.

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

Conduct – How I behave online

- I will keep my logins and passwords secret;
- I will only use the school's computers for schoolwork and homework;
- I am aware that some websites and social networks have age restrictions and I will follow those rules;
- I will not attempt to visit internet sites that I know to be banned by the school;
- I will not take part in cyberbullying by being unkind, spreading untrue rumours about others or sharing their private information without permission.

Contact – Who I message/email and how I use digital communication

- I will only e-mail or personal message people I know, or a responsible adult has approved;
- The messages I send, or information I upload, will always be polite and sensible;
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission;
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.

Content – What I use and share online

- I will not bring files into school without permission or upload inappropriate material to the school network or VLE workspace;
- I will only edit or delete my own files and not look at, or change, other people's files without their permission;
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it;
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show an adult immediately or click the DB VLE 'Golden Whistle' button to report it.

I confirm I have read these rules and accept them; I also understand that if I break these rules, my internet and VLE access will be removed.

Name:

Signed: ***Date:***

St. Louis Catholic Academy
Fordham Road
Newmarket
Suffolk
CB8 7AA

Dear Parent/ Carer

ICT including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please do not hesitate to contact your class teacher in the first instance.

Yours sincerely

Mrs Teresa B Selvey
Headteacher

✂

Parent/ carer signature

ICT Use – Agreement and e-Safety Rules

We have discussed this and ……………………………………........(child name) agrees to follow the e-Safety rules and to support the safe use of ICT at
St. Louis Catholic Academy.

Parent/ Carer Signature ………………………..…………………………

Class …………………………………. Date ………………………………