St Luke Academies Trust

Our Lady of Walsingham Catholic Primary School

E-Safety Policy

Presented to Governors: November 2015

Adopted by Directors: November 2015

Signed . . . . . Chair of Governors

Review date: July 2016

E- Safety Policy

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Our Lady of Walsingham Catholic Primary School we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Our Lady of Walsingham Catholic Primary School.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.
"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."
From: Safeguarding Children in a Digital World. BECTA 2006

Our e-safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

Roles and Responsibilities
Governors:
Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

- Regular meetings with the e-Safety Co-coordinator/Officer.
- Regular monitoring of e-safety incident logs.
- Reporting to the Pupil Outcomes Committee

Headteachers and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community.
- The Headteacher/Senior Leaders are responsible for ensuring that the e-safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and Deputy Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The E-Safety Co-coordinator:

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new ICT (computing) curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings our SEN coordinator and individual teachers to ensure all children have equal access to succeeding in this subject.

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an e-Safety Log, which will be stored in the Headteacher's office with other safeguarding materials. The e-Safety Log will be reviewed termly by the e-Safety Co-coordinator.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

E-mail

- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:
- 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 arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Access in school to external personal e-mail accounts is not allowed.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Social Networking

- Social networking Internet sites (such as Facebook, Twitter etc) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered. Children in Our Lady's are too young to be using social networking sites.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Reporting

All breaches of the e-safety policy need to be recorded in the E-Safety reporting book that is kept in the Headteacher's office. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Teachers immediately – it is their responsibility to decide on appropriate action not the class teachers.

Allegations involving staff should be reported to the Headteacher.
Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, Childline)

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office at 8:45 and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use the school phone to contact parents.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.

- Staff may use their mobile phones in the staffroom/one of the school offices.
- Parents cannot use mobile phones on school trips to take pictures of the children
- On trips staff mobiles are used for emergency only

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.
- The Headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

Staff should always use a school camera to capture images and should not use their personal devices.

Photos taken by the school are subject to the Data Protection act.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- The Headteachers or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Website.
- Work will only be published with the permission of the pupil.
- Parents should only upload pictures of their own child/children onto social networking sites.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.
- E-safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act

Assessing Risk
The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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 shall be dealt with in accordance with school child protection procedures.

Communication of Policy
Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on sites. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

- All staff will be given the School e-safety Policy and its importance explained.

Parents:

- Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.

Appendix 1

For learners in KS1
I want to feel safe all the time.
I agree that I will:

1. **always keep my passwords a secret**
2. **only open pages which my teacher has said are OK**
3. **only work with people I know in real life**
4. **tell my teacher if anything makes me feel scared or uncomfortable on the internet**
5. **make sure all messages I send are polite**
6. **show my teacher if I get a nasty message**
7. **not reply to any nasty message or anything which makes me**
8. **feel uncomfortable**
9. **not give my mobile phone number to anyone who is not a**
10. **friend in real life**
11. **only email people I know or if my teacher agrees**
12. **only use my school email**
13. **talk to my teacher before using anything on the internet**
14. **not tell people about myself online (I will not tell them my name, anything about my home and family and pets)**
15. **not upload photographs of myself without asking a teacher**
16. **never agree to meet a stranger**
17. **Anything I do on the computer may be seen by someone else.**
18. **I am aware of the CEOP report button and know when to use it.**

Signed ……..

Appendix 2

For learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school unless I am given permission
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school
- only use email which has been provided by school
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- only create and share content that is legal

Signed…….

Signed…….

Appendix 3 – Parent letter – Internet/e-mail use

Our Lady of Walsingham Catholic Primary School

Dear Parents

Please read the following letter below so that you are aware of our policy surrounding e-safety and keeping your child safe whilst on line. Please sign and return the form to school as soon as possible.

Name of child(ren)	Class teacher's name

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet and other ICT facilities at school. I know that my child has signed a form to confirm that they will keep to the school's rules for responsible ICT use. I also understand that my son/daughter may be informed, if the rules have to be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service; secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community

Parent's signature:…… Date:…….