St. Luke's Catholic Primary School

E-Safety Policy

Agreed and adopted by Governors: 24th March 2017
Written By: Stacey Beale 21st March 2017

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, bullying and for child protection.
The school's ICT Co-ordinator will also act as E-Safety Coordinator.
Our e-Safety Policy has been written by the school, building on CEOP, NSPCC and government guidance. It has been agreed by senior management and approved by governors. The E-Safety Policy and its implementation will be reviewed biannually.
Our E-safety policy should be viewed and used in conjunction with the school's ICT acceptable use policy adopted from the LA – neither policy should be used without reference to the other.

Teaching and Learning

The Byron Review "Safer Children in a Digital World" stressed the role of schools:
"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

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 children 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.

Internet use will enhance learning

The school Internet access is designed expressly for pupil use and includes 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.

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.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about e-safety incidents.

Headteacher and Senior Leaders

• The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community.
• The Headteacher and Senior Leadership Team 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.

E – Safety Co-ordinator

• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / 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 the Local Authority
• liaises with T and W ICT technical staff
• liaises regularly with ICT link governor to discuss current issues, review incident logs and filtering / change control logs

Technical staff

The Local Authority and ICT Technician are responsible for ensuring:
• that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
• that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance
• that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
• that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
• that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator
• that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

are responsible for ensuring that:
• they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
• they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
• they report any suspected misuse or problem to the E-Safety Co-ordinator or other member of the Senior Leadership Team
•digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level *and only carried out using official school systems*
• e-safety issues are embedded in all aspects of the curriculum and other school activities
• pupils understand and follow the school e-safety and acceptable use policy
• they monitor ICT activity in lessons, extra curricular and extended school activities

• they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
• in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated person for child protection / Child Protection Officer

should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:
• sharing of personal data
• access to illegal / inappropriate materials
• inappropriate on-line contact with adults / strangers
• potential or actual incidents of grooming
• cyber-bullying

Pupils

• are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they and/or their parents will be expected to sign before being given access to school systems.
• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
• will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
• should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature.*
Parents and carers will be responsible for:
• endorsing (by signature) the Student / Pupil Acceptable Use Policy
• accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Community/Other Users

Community users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This will be done in the following ways:

- A planned e-safety programme should be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and themed days throughout the school year e.g. Safer Internet Day
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils will be informed that internet use may be monitored
- Rules for use of ICT systems / internet will be posted in all rooms where internet devices are likely to be used and discussed with pupils on a regular basis
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). Therefore, parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site on a regular basis.

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff may identify e-safety as a training need within the performance management process.

All staff will be given the School E-Safety Policy and its importance explained.

Staff will be made aware that Internet traffic can be monitored and traced to the individual user.

• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies

• The E-Safety Co-ordinator will attend training sessions and review guidance documents released by LA and other relevant sources.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.

• Participation in school training / information sessions.

Technical - infrastructure

The school will be responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

• School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined any relevant Local Authority E-Safety Policy and guidance

• There will be regular reviews and audits of the safety and security of school ICT systems

• Servers, wireless systems and cabling must be securely located and physical access restricted

• All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded and reviewed, at least annually.
• All computers will be provided with a specific username and password which will change at least each half term.
• The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and kept in a secure place (eg school safe)
• Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
• The school maintains and supports the managed filtering service provided by TAW
• Any filtering issues should be reported immediately to TAW
• School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
• Impero remote management tool is used by staff to control workstations and view users activity
• Users are to report any actual / potential e-safety incident to the Computing Co-ordinator (using Appendix 1.of this policy) who will investigate these and decide whether to refer to the Head teacher. E-safety incidents that are of a safeguarding nature should be shared immediately with the designated persons for safeguarding (HT/ DT).
• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
• Provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system can be permitted through a temporary log on / email granted through TAW. Users must sign the AUP before this can take place.
• The school infrastructure and individual workstations are protected by up to date virus software.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

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 head teacher 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 and will only be published with parental permission.
Pupils' full names will not be used anywhere on the Web site, 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.

Social networking and personal publishing

- The school will block/filter access to social networking sites e.g. Facebook
- Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind that 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.
- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (permission signed by parents or carers at the start of the year / entry to school Reception).

Managing videoconferencing

When this becomes available within the school, videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
Pupils will be required to gain permission from the supervising teacher before making or answering a videoconference call.
Videoconferencing will be appropriately supervised for the pupils' age.

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.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. This states that data should be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
• Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
• Transfer data using encryption and secure password protected devices.
Personal data must not be stored on any portable computer system, USB stick or any other removable media.

Authorising Internet access

All staff must read 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.
Parents will be asked to sign and return a consent form.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

• In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
• Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
• It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x							x
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on mobile phones or other camera devices				x				x
Use of hand held devices eg PDAs, PSPs	x							x
Use of personal email addresses in school, or on school network	x							x
Use of school email for personal emails				x				x

When using communication technologies the school considers the following as good practice:

• The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).

• Users need to be aware that email communications may be monitored.

• Users must immediately report, to their line manager – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

• Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.

• Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff. Staff must notify their line manager asap if they receive email from parent/carer via their personal TAW email address.

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 LA can accept liability for the material accessed, or any consequences of Internet access.

It is most likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through the school behaviour policy. However, if a pupil is deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities) police advice should be sought.

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.

St Luke's Catholic Primary School

E-Safety Concerns

Date:	Time:
Children involved:	
Adults involved:	
Nature of concern:	
Action taken:	
Referral to safety co-ordinator: Date given:	
Referral to head/deputy: Date given:	
Signed: Date:	