E-safety Policy: Safeguarding our children

St Laurence Catholic Primary School

Through God's grace, a community growing in knowledge and understanding

Background to the Policy

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school:

- the ground rules we have developed in school for using the Internet and online technologies
- how these fit into the wider context of our other school policies
- the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.

Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, media and information resources, is one the school shares with parents and carers. At St Laurence Primary School, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

This policy is available:

- On school website
- Via the office
- In the school staffroom

Rationale

At St Laurence Primary school, we believe that the use of information and communication technologies in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to raise educational standards and promote pupil achievement. Yet at the same time we recognise that the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content
• Unauthorised access to / loss of / sharing of personal information
• The risk of being subject to grooming by those with whom they make contact on the internet.
• The sharing / distribution of personal images without an individual's consent or knowledge
• Inappropriate communication / contact with others, including strangers
• Cyber-bullying

• Access to unsuitable video / internet games
• An inability to evaluate the quality, accuracy and relevance of information on the internet
• Plagiarism and copyright infringement
• Illegal downloading of music or video files
• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the school. For example, school and personal data being entered on web/social networking sites, fraudulent email traps and cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision to manage the risk and deal with any threat to safety.

Teaching and Learning Using Online Technologies

The internet is a part of everyday life for education, business and social interaction.

Benefits of using online technologies in education include:

- Access to world-wide educational resources
- Inclusion in the National Education Network (NEN) connecting all UK schools and resources
- Access to experts who would otherwise be unavailable
- Access to anytime, anywhere learning
- Collaboration across schools, networks of schools and services

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. At St Laurence Primary School, we believe that a comprehensive programme of e-safety education is vital for developing our pupils' ability to use technologies safely. This is achieved using a combination of discrete and embedded activities drawn from a selection of appropriate materials (see appendices)

Our programme for e-safety education is evidenced in teachers' planning either as discrete or embedded activities. Members of staff constantly monitor pupils' use of the internet and other technologies and are able to monitor pupils' use of communication and publishing tools.

Messages involving Risks and Rules and Responsibilities are taught and/or reinforced as detailed in the school's ICT Acceptable Use Policy (AUP)

Technology in our School

The school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both E2BN and the Local Authority's Education ICT Service. The school have also had a freelance technician since 2006. E2BN is the East of England Broadband Network – one of 10 networks set up by the government to help raise standards in teaching and learning by the use of broadband technology

The Protex filtering system available from E2BN is already providing safe and secure Internet access to over 600,000 learners and library users. This DfE-approved filtering service provides age-appropriate protection from inappropriate content and a strong defence against student attempts to bypass the filter.
All Protex systems are automatically updated with the latest list and software upgrades.

From the E2BN website (accessed 08.03.2017) http://protex.e2bn.org/cms/home.html

This helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. If / when they do, the school's AUPs and e-safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

Technologies regularly used by pupils and adult stakeholders include:

Staff use:
- computers
- mobile phones
- personal devices eg tablets
- cameras
- CD players
- Interactive White Board (IWB) displays
- Sound systems
- Projector

Pupils use:
- computers
- devices for programming
- keyboards
- cameras
- tablets

Others on school premises:
- Sound systems
- Computers
- IWB displays
- Projector

Whilst we recognise the benefits of individual pupil logins to our school network, we prefer to use year group logins for ease of access.

All members of staff have individual, password protected logins to the school network and visitors to the school can access part of the network using a generic visitor login and password.

Safeguarding Our Children Online

St Laurence Catholic Primary School recognises that different users will be expected to use the school's technology systems in different ways – appropriate to their age or role in school. We acknowledge the need to:

Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.

UKCCIS – June 2008

The school has published Acceptable Use Policies (AUPs) for pupils and staff; pupils and staff all sign to indicate their acceptance of our AUPs and of relevant sanctions which will be applied should rules be broken. Parents are encouraged to view the pupils' AUPs on the e-safety page of the school website.

The following is a summary of some of the key messages held within our AUPs. Please see our ICT Acceptable Use Policy for full details.

<u>Pupil use:</u>
- Filtered internet with adult present
- E-safety cadets' software
- A reporting system for concerns/inappropriate material

Adult Use:

- Filtered internet
- Occasional personal use of technology
- Password and usernames kept safe

Any known or suspicious online misuse or problem will be reported to the designated E-Safety Co-ordinator for investigation/ action/ sanctions. The school will keep evidence and/or contribute to a log of any 'extreme' or 'unusual' actions that a pupil has been involved in online. This log will be used to keep track of the child's behaviours over the entire time they are at the school and will be stored alongside other incident logs. These are stored securely by the head teacher.

Responding to Incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond to if an e-safety incident occurs or they suspect a child is at risk through their use of technology. Responding to an e-safety incident in school is no different to responding to other incidents in school.

If an e-safety incident occurs St Laurence Catholic Primary School will follow its usual procedures for dealing with other incidents including internal sanctions and involvement of parents (for ICT, this may include the deactivation of accounts or restricted access to systems as per the school's AUPs). Where the school suspects that an incident may constitute a Child Protection issues, the usual Child Protection procedures will be followed:

Dealing with Incidents and Seeking Help
If a concern is raised, refer immediately to the designated person for child protection. If that is not possible refer to another member or the Senior Management Team or, if necessary, the Chair of Governors.
It is their responsibility to:

Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator
Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If in doubt, they will consult the Education Child Protection Service helpline -
Step 3: Ensure that the incident is documented using the standard child protection incident logging form (see Safeguarding & Child Protection Policy)

Depending on the judgements made at steps 1 and 2 the following actions should be taken
Staff instigator – follow the standard procedures for Managing Allegations against a member of staff. If unsure seek advice from the Local Authority Designated Officer or Education Officer.
Staff victim – Seek advice from the school's HR provider and/or Educational Child Protection Service

Illegal activity involving a child – refer directly to Cambridgeshire Constabulary by phoning 101 - make clear that it is a child protection issue
Inappropriate activity involving a child – follow standard child protection procedures. If unsure seek advice from Education Child Protection Service helpline: 01223 703800

Equally, if the incident involves or leads to an allegation against a member of staff, the school will follow the usual procedures for dealing with any allegation against a member of staff (see appendix).

Terms used in this policy

AUP: Acceptable Use Policy.
A document detailing the way in which new or emerging technologies may/may not be used – may also list sanctions for misuse.

Child: Where we use the term 'child' (or its derivatives), we mean 'child or young person'; that is anyone who has not yet reached their eighteenth birthday.

E-safety (or online safety): We use e-safety, and related terms such as 'online safety', 'communication technologies', and 'digital technologies' to refer to all fixed and mobile technologies that children may encounter, now and in the future, which might pose e-safety risks. We try to avoid using the term 'ICT' when talking about e-safety as this implies that it is a technical issue – which is not the case. The primary focus of e-safety is child protection: the issues should never be passed solely to technical staff to address.

PIES: A model for limiting e-safety risks based on a combined approach to policies, infrastructure and education, underpinned by standards and inspection.

Safeguarding: Safeguarding is defined (for the purposes of this document) as the process of increasing resilience to risks when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection. E-safety is just one aspect of a much wider safeguarding agenda within the UK. Those with responsibility for the development and delivery of e-safety policies should embed their work within the wider safeguarding agenda, and work across services to ensure that they are delivering the best possible opportunities for the children and young people in their care.

Users: We use this term, and related terms such as service users and end users, to mean those people who will ultimately be bound by the provisions of an **AUP**

Policy Reviewed and shared with staff: December 2015
Ratified by Full Governing Body: 28th January 2016
Updated and re-ratified by Full Governing Body: 16th March 2017
Next review due: March 2018
This policy has undergone an Equality Impact Assessment

Appendix: List of Relevant Policies and Documents:

- Data Protection Policy
- County guidance (e.g. Use of Digital Images, e-mail)
- Safeguarding Child Protection Policy
- AUPs- staff, pupil, parents
- Anti-Bullying Policy
- School Complaints Procedure
- LA Infrastructure guidance (E2BN)
- Risk assessment log
- Incident Log
- PSHE Policy
- Behaviour Policy
- Computing Policy
- Starz letter to parents
- County Guidance regarding Allegations against a member of staff
- Prevent duty and school's Prevent Action Plan

Policy Name: **E-Safety**
Policy Date: 16/03/2017

EQUALITY IMPACT ASSESSMENT for SCHOOL POLICIES

		Yes / No	Comments
1.	Does the Policy/Guidance affect one group less or more favourably than another on the basis of:		
	• Age (for policies affecting staff)	N/A	
	• Disability	N	
	• Sex	N	
	• Gender reassignment	N	
	• Pregnancy/maternity	N	
	• Race (which includes colour, nationality and ethnic or national origins)	N	
	• Sexual orientation	N	
	• Religion or belief	N	
	• Marriage / civil partnership	N	
2.	Is there any evidence that some groups are affected differently?	N	
3.	If we have identified potential discrimination are any exceptions reasonable, legal and justifiable?	N/A	
4.	Is the impact of the policy/guidance likely to be negative?	N	
5.	If so, can the impact be avoided?	N/A	
6.	What alternatives are there to achieving the policy/guidance without the impact?	N/A	
7.	Can we reduce the impact by taking different action?	N/A	
8.	Is the policy compliant with Prevent requirements?	Y	

Equality Impact Assessment carried out by: M J O'Sullivan/Full Governing Body

Date: March 2017