WRITTEN WITH GUIDANCE FROM LANCASHIRE SCHOOLS' ICT CENTRE

St John's Catholic Primary School

E-Safety Policy

January 2023

The implementation of this policy will be monitored by SLT and Subject Leaders and any other relevant staff.

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective e-safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact. It will also ensure that all areas of the Every Child Matters agenda are covered.

Our e-safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community is prepared to deal with the safety challenges that the use of technology brings.

2. Our school's vision for e-Safety

Our school provides a diverse, balanced and relevant approach to the use of technologies, especially as the children move further up the school. Children are encouraged to maximise the benefits and opportunities that technology has to offer.

As a whole staff we ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively. All the children throughout school are aware of the SMART rules. Following these rules ensures that children are equipped with the skills and knowledge to use technology appropriately and responsibly.

School does teach how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment in ICT, PSHE and SEAL lessons.

All users in our school community understand why there is a need for an e-safety.

3. The role of the school's e-safety Champion

Our e-safety Champion is Elizabeth Devey
The e-safety Champion is the nominated point of contact within the school for e-safety-related issues and incidents. However, certain responsibilities may need to be delegated to other staff e.g. Subject leader or Designated Senior Person/Child Protection Officer as is necessary.
The role of the e-safety Champion should include:
Having operational responsibility for ensuring the development, maintenance and review of the school's E-safety Policy and associated documents, including:

• Acceptable Use Policies.
• Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
• Ensuring all staff are aware of reporting procedures and requirements should an e-safety incident occur.
• Ensuring any e-safety Incident is logged.
• Keeping personally up-to-date with e-safety issues and guidance through liaison with the Local Authority Schools ICT Team and website and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP). This will be updated on the school website and reported to parents where relevant.
• Providing or arranging e-safety advice/training for staff, parents/carers and governors.
• Ensuring the Head teacher, SLT, staff, pupils and governors are updated as necessary.
• Liaising closely with the school's Designated Senior Person / Child Protection Officer (CG)

4. A co-ordinated approach across relevant safeguarding areas.

4 Security and data management

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school.

This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- And importantly, only transferred to others with adequate protection.
- In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

Use of mobile devices:

Pen drives, laptops, mobile phones, games consoles, Digital Cameras, Voice recording devices, etc.

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:
• That some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered internet content.
• That any devices used outside of school are virus checked before use on school systems.

Mobile telephones:

Mobile phones are not permitted in school for children's use. Any brought to school will be stored in the safe until the end of the day. Staff should ensure their own phones are turned off/silent and not used in the classroom. Sending text messages and making phone calls should, wherever possible, be avoided in the staff room as a common courtesy to other staff room users.

It is acceptable to use personal mobile phones for school activities e.g. school trips.

A school mobile phone is made available for activities where a personal mobile phone maybe considered inappropriate, i.e. Out of School club and school kitchen for emergency calls. Staff should be familiar with guidance from safeguarding team (see staff handbook).

Other Mobile devices:
Children are not permitted to bring pen drives into school. Where staff use these devices they should be virus checked before information is transferred to the school system.
Images should only be taken with school cameras/iPads.

Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.
As photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (1998), school must have written permission for their use from the individual and/or their parents or carers.
Staff and pupils are aware that full names and personal details will not be used on any digital media, particularly in association with photographs. Children's first name and surname will never be used on the website with a photo of just one child and where possible one child photos will be bunched together.
Parents/carers, who have been invited to attend school events, are allowed to take videos and photographs, but are asked not to publish them online or on personal websites where anyone can view them.
All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites and are asked to keep their pages private and not available for public viewing.
Staff should use only school cameras to take pictures of the children and when taking photographs/video and will ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
All staff, parents/carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.

Images taken must be transferred as soon as possible to the secure school drive and removed from any mobile device. Photos taken in school must not be taken out of school on mobile devices.

Video conferencing:

The relevant permissions letter is made available for parents/carers to sign giving permission for their child/children to participate in video and photographs. Children should never be appearing 'live' on the Internet through a video conferencing link without a member of staff present at all times. It is still important to remember that the images which are broadcast from school could be captured as a snapshot or video clip from a system receiving the broadcast.

Approval by the Head teacher must be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.

Communication technologies

In our school the following statements reflect our practice in the use of email.
It is recommended that all users have access to the Lancashire Grid for Learning service as the preferred school e-mail system. Our ICT subject technician or head is able to set up new accounts for both staff and pupils.
Only official email addresses should be used to contact staff/pupils.
The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Westfield Centre.
All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
All users, both staff and/or pupils, must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

In our school the following statements outline what we consider to be acceptable and unacceptable use of

Social Network sites:

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Face book, Twitter and Club Penguin. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments.

NB: LCC safeguarding guidance is shared with staff.

Many Social Network sites have age restrictions for membership e.g. Face book's minimum age is 13 years old.

All staff need to be aware of the following points:

• They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
• Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
• If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
• Pupils and parents must never be added as 'friends' on any Social Network site.
• Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

In our school the following statements outline what we consider to be acceptable and unacceptable use of

Instant Messaging:

This is a popular tool used by adults and pupils that allows 'real time' communication and often integrates the ability to transmit images via a webcam. Although these sites are 'blocked' for use in Lancashire schools by default, some exceptions are made, see video conferencing.

Staff and children are aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts through-safety lessons/training.

Websites and other online publications:

Lots of work and constant updates occur on our school website. It has been a useful tool to point parents to different outside agencies. It is ensured that our school website is effective in communicating e-safety messages to parents/carers.

Everyone in the school is made aware of the guidance for the use of digital media on the website, only staff are allowed to edit the website.

It is made clear there are to be no pictures linked to full names.

Content is always considered subject to copyright/personal intellectual copyright restrictions.

All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with broadcastings.

Others:

As we risk assess and introduce new technologies we will need to update our policy to reflect what we consider to be acceptable and unacceptable use of these.

Dealing with incidents

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher who must refer this to external authorities, e.g. Police, CEOP, and Internet Watch Foundation (IWF).

We will never personally investigate, interfere with or share evidence as we may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident (http://www.iwf.org.uk) .These groups are licensed to investigate – schools are not!

Examples of illegal offences are:

• Accessing child sexual abuse images
• Accessing non-photographic child sexual abuse images
• Accessing criminally obscene adult content
• Incitement to racial hatred
It is more likely that school will need to deal with incidents that involve inappropriate rather than illegal misuse.

It is important that any incidents are dealt with quickly and actions are proportionate to the offence. Some examples of inappropriate incidents are listed below with suggested sanctions.

Incident Procedure and Sanctions

• *Accidental access to inappropriate materials.*

Minimise the webpage/turn the monitor off then tell a trusted adult.
Enter the details in the school Incident Log and report to LGfL filtering services, if necessary.
Persistent accidental offenders may need further disciplinary action.

• *Using other people's logins and passwords maliciously.*

Inform SLT or designated e-safety Champion.
Enter the details in the Incident Log.
Raising awareness of e-safety issues and the AUP with individual child/class.
More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.
Consider parent/carer involvement.

• *Deliberate searching for inappropriate materials.*

Inform designated e-safety Champion.
Enter the details in the Incident Log.
Raise awareness of e-safety issues and the AUP with individual child/class.
More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.
Consider parent/carer involvement.

• *Bringing inappropriate electronic files from home.*

Consider parent/carer involvement.

- *Infrastructure and technology*

As a school, we are responsible for ensuring that our infrastructure /network are as safe and secure as possible.

Pupil Access: Pupils can only log onto a computer with their year group domain user name and password. Administrator passwords are changed yearly.
Software/hardware: Our IT technician regularly updates computers and checks hardware.
Managing the network and technical support: BT is the current Lancs provider of I.T.
Filtering and virus protection: All our computers are Sophos protected and are filtered and monitored through LGfL . See information and access security policy.

Education and Training

Education and training are essential components of effective e-safety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. E-safety guidance must be embedded within the curriculum and advantage taken of new opportunities to promote e-safety. This can be done through discreet IT lessons, SEAL or PSHE.

- *e-safety across the curriculum*

All staff are expected to promote and model responsible use of ICT and digital resources. Regular updates on e-safety Policy, Acceptable Use Policy, curriculum resources and general e-safety issues are discussed in staff and SLT meetings.

- *e-safety – Raising staff awareness*

All staff made aware of this policy through staff handbook.

E-safety – Raising parents/carers awareness

“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.” (Byron Report, 2008).

Our school offers regular opportunities for parents/carers and the wider community to be informed about e-safety, including the benefits and risks of using various technologies through notes for parents on the ‘Parents page’ of the website and guidance from CEOP.
Parents are given the opportunity to attend e-safety Awareness sessions and teachers can give appropriate advice where appropriate.
There is some promotion of external agencies advice on our website, which will need to be regularly checked for relevance.

- *e-safety – Raising Governors’ awareness*

Governors are to be made aware of this policy and any updates via governor meetings.

Standards and inspection

As a school we should consider on a regular basis:

• How will we know if our e-safety policy is having the desired effect?
• How are e-safety incidents monitored, recorded and reviewed?
• Who is responsible for monitoring, recording and reviewing incidents?
• Is the introduction of new technologies risk assessed?
• Are these assessments included in the e-safety Policy?
• Are incidents analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children? How can these patterns be addressed most effectively e.g. working with a specific group, class assemblies, reminders for parents?
• How does the monitoring and reporting of e-safety incidents contribute to changes in policy and practice?
• How are staff, parents/carers, pupils and governors informed of changes to policy and practice?
access to the myLGfL filtering interface (e.g.head@exampleschool.lancs.sch.uk).