St. Gregory's
Catholic Primary School

eSafety Policy

2019 - 20

School Mission Statement

"In the joy of the Gospel

We will work together

To be kind, fair and honest,

And become the people Jesus calls us to be."

Policy Development

This policy has been written using information and advice from The Lancashire eSafety Framework Document and The Lancashire e-Safety Guidance Document.

This eSafety Policy forms part of our commitment to The Lancashire eSafety Charter.
For further information about the Lancashire's eSafety Charter. Please see
http://www.lancsngfl.ac.uk/esafety

This eSafety Policy has been written as part of a consultation process involving: Mr Wilson (Computing and e.Learning Leader), Mr Darbyshire (Head Teacher), Mrs Wilson (Acting Deputy Head). Margaret Scard Chair of Governors

Policy Monitoring and Review

Mr Darbyshire and Mr Wilson are responsible for ensuring that this policy is monitored. It will be reviewed annually by the Governing Body.

October 2019

St. Gregory's Catholic Primary School e-Safety Policy 2016/17

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 eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our eSafety Policy, as part of a wider safeguarding agenda, outlines how we will ensure member of our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

2. Our vision for eSafety

Our school aims to provide a diverse, balanced and relevant approach to the use of I.C.T. to prepare the children for the demands of current and future technology. Children are encouraged to maximise the benefits and opportunities that technology can provide whilst creating a safe and secure learning environment. To promote such an environment, the children are equipped with the skills and knowledge of being safe online from the EYFS and KS1 through to the end of KS2 and beyond. They are encouraged to independently assess and recognise the risks associated with technology and how to deal with them both within and outside the school environment.

3. eSafety Champion

St Gregory's eSafety Champion is Mr Darbyshire. He is able to undertake this role as he holds a senior leadership position and is also a class teacher in school.

The core duties of his role are:

- Having operational responsibility for ensuring the development, maintenance and review of the school's eSafety 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 eSafety incident occur.
- Ensuring the eSafety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with eSafety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging eSafety advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Leader, Mrs Wroblewski, to ensure a co-ordinated approach across relevant safeguarding areas.

4. Policies and Practices

This eSafety policy should be read in conjunction with all our other policies and documents, but in particular:

Child Protection Policy, Behaviour for Learning Policy, Anti-bullying Policy, Code of Conduct, Acceptable Use Policy and Staff Handbook.

4.1 Security and Data Management

We take seriously our responsibility for the management of potentially sensitive data.

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:

Key information/data is mapped and securely stored on the main office and Headteacher office computers. This is only accessible by the School Business Manager, Office Admin Assistant and Headteacher.

The Headteacher has overall responsibility for managing all information.

Staff have been informed of the location of all data relevant to them by the Headteacher.

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
- Only transferred to others with adequate protection.

Our school ensures that data is kept appropriately and managed both within and outside the school in the following ways:

- School's equipment, including teacher laptops, must only be used for school purposes and must not contain personal information e.g. personal images, personal financial details, music downloads, personal software. Computers are also accessed using a safe username and password and it is the responsibility of each individual to keep this secure at all times. Any breaches in security must be reported immediately to Mrs Wroblewski.

- School equipment must not be used, for online gambling, dating websites, home shopping, holiday booking, and social networking either in school or at home.

- Staff are aware of the school's procedures for disposing of sensitive data, such as shredding hard copies, deleting digital information, deleting usernames and passwords from school's VLE, deleting email accounts, IEP, PIPs and SATs information.

- There is a shredder in the school office to ensure there is always availability for safe disposal of documents. Each staff member is responsible for the disposal of documents securely. School data if stored on memory sticks, must be password protected and remain in school.

4.2 Use of Mobile Devices and Telephones

In our school, we recognise the use of mobile devices can offer a range of opportunities to extend children's learning. However, the following statements must be considered when using devices:

- Children are not allowed to use mobile personal devices in school (unless they are given prior permission by a member of staff in exceptional circumstances).

- Children who have to bring mobile telephones into school (for example those walking home from school alone) must give them to the class teacher at the start of the school day. They are locked away securely until the end of the day. This will only apply to children in Y5 and Y6.

- Staff and other adults working in school or visitors to school are not allowed to use personal mobile telephones in classrooms or other teaching areas or toilet areas. They can only be used in the staffroom or office areas where there are no children present. This is due to the fact that most mobile telephones contain a camera facility and this forms part of our safeguarding practice.

- Parents and carers are permitted to record school events but are always reminded that this must be for personal use only and not shared on social media sites.

- Staff at St Gregory's have been provided with lockers to ensure the secure storage of valuables such as mobile phones whist at work.

- School iPads are available to the children to use, under the direction and supervision of the class teacher or teaching assistant.

- An iPad Mini is available for every class teacher to use in school or on school visits for the purpose of recording and uploading images and clips to the school website or blogs or for learning records. These devices are not for pupil use. Once images have been uploaded or stored in the secure staff drive for use

in promotional school materials they must be deleted from the device. Images of children will be deleted once they leave the school.

4.3 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.

All users of digital media (photographs, video) in our school are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media.

Generic parental consent to use children's images within the school, as well as in brochures or on the school blogs or website is obtained on a regular basis and kept securely in the school bursar's office.

Full names and personal details are never used on any digital media.

Parents and carers using digital media to record images at school events are always cautioned to record their own children as far as practicable and not to publish any on Social Networking sites or to circulate images.

All staff are aware that personal equipment must not be used to store digital content.

All members of staff should consider their position of responsibility and adhere to professional standards and consider the risks of publishing images to personal Social Network sites. This is covered in the Staff Handbook Safe Practice section.

Any photos or videos taken by staff are for school purposes alone such as school website images to illustrate the curriculum, prospectus, display or for pupils' learning records. Once printed or uploaded they must be deleted from the device. Personal equipment must not be used for this purpose, only school devices.

When taking photographs or video, staff will ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted. The context of the learning should be clear from the picture.

4.4 Communication Technologies

All school digital communications should always be professional in tone and content.

Email:

Email is not used for parent-teacher or pupil-teacher communication. Any parents or pupil wishing to make contact with the class teacher may do so via the Head Teacher's email.
Every class has a secure blog forum via which children and their parents or carers are able to make contact with the class teacher. Content is screened by staff before it is approved for publication online.

In our school the following statements reflect our practice in the use of email:

- The Lancashire Grid for Learning (My LGfL) service is the preferred school e-mail system for use by members of staff.
- Any incidents of SPAM on the LGfL email service 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.
- In addition, 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 must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- The school includes a standard disclaimer at the bottom of all outgoing emails as follows:

School e-mail disclaimer:
This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent St. Gregory's Catholic Primary School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

Social Networks:

As part of the Acceptable Use Policy, all staff sign up to the following rules:

- Adults working in school, whether paid or voluntary, are not allowed to communicate with pupils using and digital technology where the content of the communications may be inappropriate or misinterpreted.
- Adults in school are NOT permitted to add pupils or past pupils as 'friends' on Social Networking sites.
- Children are given guidance on the age restrictions of certain Social Networking sites and educated about the need to keep themselves e-safe.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Whatever means of communication is used; staff should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever. See Staff Handbook.

Many adults and pupils regularly use Social Network sites, e.g.Club Penguin, Moshi Monsters, Facebook or Twitter, although the minimum age for registering for some of these excludes primary school pupils. These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute. We view any comments of this nature made by staff or pupils as being unacceptable use of such resources outside school and in complete contravention of our school motto and code of conduct. The school reserves the right to take appropriate steps in the event that any complaint is made in relation to this.

Virtual Learning Environment (VLE) / Learning Platform:

In our school, safe and responsible use of the VLE (Moodle) is ensured. The following statements outline what we consider to be acceptable and unacceptable use of Virtual Learning Environments:

- Members of staff are given access to edit and add appropriate content to their own year group with the exception of the ICT Coordinator and SMT who are granted administration access to the whole school VLE.
- Children are each issued with a username and password.
- The mutual privacy of these is agreed upon in accordance with the e-safety education values taught in school.
- Children are not permitted to share their personal data with others.
- The removal of out expired accounts is maintained and monitored by the Computing and eLearning Leader and SLT.

Web sites and other online publications:

Our school website and other online publications, e.g. podcasts and blogs, provide an effective way to communicate information. In our school, the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

- esafety information is provided to parents and carers on the school website.
- All staff members are made aware of the guidance for the use of digital media/personal information on the school website in accordance with the Staff Acceptable Use Policy (AUP) and the Data Protection Act (1988)
- Information is monitored and maintained by the Computing and eLearning Leader, Chair of Governors and the SLT.
- Wherever possible, downloadable materials are in a read-only format (e.g. PDF) to prevent content being manipulated and potentially re distributed without the school's consent.

4.5 Acceptable Use Policy (AUP)

The school has a number of AUPs for staff, children and parents, carers and visitors.

Our policies are intended to safeguard that all users of technology within school will be responsible and stay safe. It is in place to ensure that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

If for any reason, any children are not granted access to technology in school a list will be kept and made available to staff.

In addition to these agreements, the school will provide e-safety education opportunities for staff, parents, carers and children on site and online.

4.6 Dealing with Incidents

As a staff we have considered the incidents that may occur in school and have agreed a plan of action that each member of staff will follow. Please see below. eSafety infringements of a minor nature are dealt with by members of staff in the classroom.

A major breach of the rules has to be reported to the eSafety champion, the Headteacher and logged in the eSafety incident log which is situated in the school office.

Any incidents will be monitored and audited on a regular basis by the e-safety Champion and the SMT.

Inappropriate Incidents:

Accidental access to inappropriate materials.	• Minimise the webpage/turn the monitor off. • Tell a trusted adult. • Enter the details in the 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 eSafety Champion. • Enter the details in the Incident Log. • Additional awareness raising of eSafety 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.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

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

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

Infrastructure and technology:

Our school subscribes to the Lancashire Grid for Learning/CLEO Broadband Service where internet content filtering is provided by default. The filtering service provides a high level of protection, but all staff members are made aware of eSafety issues and children may not access potentially harmful sites (like Google images or games sites) without adult consent.

Sophos Antivirus software is installed on all computers that access the school server.

Pupil Access:

- Children are always supervised when using technology in school.
- Children must seek adult supervision before accessing online materials.
- All staff will check any website they direct the children to for an independent task before the lesson to ensure all content and links the website may take you to are acceptable.

Passwords:

- All staff are aware of the guidelines in the Lancashire ICT Security Framework for Schools (www.lancsngfl.ac.uk/esafety)
- All users of the school network have secure usernames and passwords.
- The administrator password for the school network is only available to the ICT technician and the eSafety champion and is kept safe by the eSafety champion.
- All staff and pupils are regularly reminded to keep passwords secure.
- Passwords for school systems are created by individuals and known only to individuals concerned.

Software/hardware:

- The school has legal ownership of all software.
- Software licences are kept in the school bursar's office.
- Equipment is regularly audited and records are kept in the school bursar's office.
- Software installation is only carried out by the school ICT technician who is monitored by senior members of staff.

Managing the network and technical support:

- All servers, wireless systems and cabling are securely located and physical access is restricted. Servers are backed up every evening.
- All wireless devices are security enabled.
- All wireless devices are only accessible through a secure password known only to the school ICT technician.
- Security for the school network is provided by the Lancashire School's ICT centre and our designated school ICT technician.
- Safety and security of our school network is reviewed regularly by the school ICT technician.
- School systems are kept up to date and updated with critical software updates/patches on a regular

basis by the school ICT technician who visits the school on a weekly basis.

- All users (staff, pupils, guests) have clearly defined access rights to the school network. Staff and pupils each have their own designated password to access the school network; guests
- Staff and pupils are required to log out of a school system when a computer/digital device is left unattended.
- No users are allowed to install executable files or install software – this is only done by the school's ICT technician during his weekly visits.
- Users report any suspicion or evidence of breaches of security to the eSafety champion and the school ICT technician who attends to it.
- Each teacher has a designated laptop for use for planning purposes.
- Staff are aware that teacher laptops are school property and that they must not be used to store or download excessive or inappropriate content of a private nature.
- All internal/external technical support providers are aware of our school's requirements and standards regarding eSafety.
- The school Computing and eLearning Leader and also the school eSafety champion are responsible for liaising with and managing technical support staff. They are also responsible for communicating any issues to the Governing Body.

6. Education and Training

Education and training are essential components of effective eSafety provision. It is important to quip individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and teach them effective ways to deal with them is fundamental. eSafety guidance is embedded within the new curriculum for 2014 and advantage is taken of new opportunities to promote eSafety. This section of the policy outlines how eSafety messages are communicated to the various stakeholder groups in our school community.

6.1 e Safety across the curriculum

We provide regular eSafety teaching to staff and pupils via our ICT curriculum. There is an additional focus on eSafety during 'Safer Internet Day' and during Anti-Bullying Week. Children with special educational needs are made aware of how to keep themselves eSafe. Pupils are taught about Data Protection and Copyright Legislation. Pupils are taught to critically evaluate materials and develop good research skills. eSafety rules are displayed in classrooms and designated areas to keep children safe.

6.2 e Safety – Raising staff awareness

All staff are regularly updated on eSafety via staff meetings. The school's eSafety Champion provides guidance and training as when required.

6.3 e Safety – Raising parents/carers awareness

Parents/carers are regularly updated about eSafety via the weekly school newsletter and annually via the

Acceptable Use Policy for Parents and Carers and eSafety workshop.

6.4 e Safety – Raising Governors' awareness

Governors are regularly updated about eSafety via the weekly school newsletters and annually via the school's eSafety Policy. They are also invited to attend the eSafety workshop.

7. Standards and inspection

The effectiveness of our eSafety Policy is monitored by the eSafety champion, Computing and eLearning Leader leader and every member of staff in our school. Any incidents are recorded and analysed to ensure any issues do not become a greater issue. Any new technologies are risk-assessed before installation by the school ICT technician and monitored by members of staff.

Policy approved 13.10.19