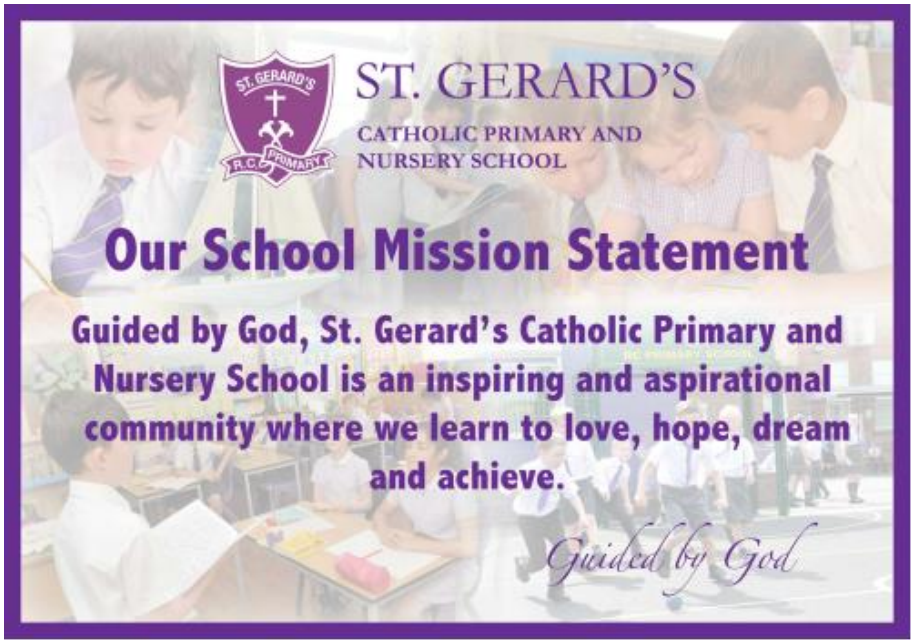
St Gerard's Catholic Primary and Nursery School

E-Safety Policy

Agreed by Governors November 2016
Signed (Chair of Governors) Ms Sharon Miller



SAFEGUARDING STATEMENT

"St Gerard's Catholic Primary and Nursery School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment".

E-safety Policy

"When online, children and young people can learn new things, get help with homework, express themselves creatively and connect with friends and family.

There are also risks, but by understanding and talking about the dangers you can help keep your child safe online."

(www.nspcc.org.uk)

Policy Date:	**October 2016**
Policy Status:	**Statutory**
Policy Review Cycle:	**Biannual**
Next Review Date:	**October 2018**

Rationale:

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school E-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, 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.

Many of these risks reflect situations in the off-line world and it is essential that this E-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The E-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Key Responsibilities

Headteacher:

- The Headteacher is responsible for ensuring the safety (including E-safety) of members of the school community, though the day to day responsibility for E-safety will be delegated to the E-safety Co-ordinator
- 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 Senior Leadership Team/Senior Management Team will receive regular monitoring reports from the E-safety Co-ordinator

Governors:

- To ensure that the school has in place policies and practices to keep the children and staff safe online
- To approve the E-safety and review the effectiveness of the policy
- To support the school in encouraging parents and the wider community to become engaged in online safety activities

Teaching and Support Staff:

- To embed online safety in the curriculum
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually.
- To report any suspected misuse or problem to the online safety coordinator
- To maintain an awareness of current online safety issues and guidance e.g. through CPD
- To model safe, responsible and professional behaviours in their own use of technology

Pupils:

- Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school
- To contribute to any 'pupil voice' / surveys that gathers information of their online experiences

Parents/Carers:

Many parents and carers have only 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/regulation of the children's online 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. The School will seek to inform parents about E-safety and to provide support and guidance. Parents can also support by doing the following:

- To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/children
- to consult with the school if they have any concerns about their children's use of technology
- to support the school in promoting online safety and endorse the Home/School Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images

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.
- E-safety should be taught regularly through a scheme of work with identified progression of knowledge, skills and understanding.
- E-safety skills should be embedded through both discrete Computing and cross-curricular application.
- In lessons where internet use is pre-planned, it is best practice that 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites visited.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online 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.

Technical-infrastructure/equipment, filtering and monitoring:

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the E-safety technical requirements outlined by the Acceptable Use Policy and LA requirements
- School ICT systems must be regularly updated to ensure up-to-date anti-virus definitions and Microsoft Windows Security Updates are installed. Essential software i.e. Acrobat Reader, Flash Player, Java, Internet Explorer, iTunes etc. must be kept current
- 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 by the Network Manager and will be reviewed, at least annually, by the Computing Coordinator
- All users will be provided with a username and password to access the school network by Technical staff who will keep an up to date record of users and their usernames
- All users of the school website (staff and pupils) will be provided with a username and password for secure access in school and beyond
- The "administrator" password for the school ICT system, used by the Computing Coordinator and Technical Staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- School Data should be securely managed when taken off the school site using encrypted memory devices or password protected files
- 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 Halton Borough Council
- In the event of the Technical Staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader)

Use of digital and video images:

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:

- 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 e.g. 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.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Photographs will not be named and in other places, no full names will be used on the website.

Communication:

The policy will be communicated to staff/pupils/parents/carers in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Regular updates and training on online safety for all staff
- Acceptable use agreements discussed with staff and pupils at the start of each year
- Acceptable use agreements to be issued to whole school community, on entry to the school

School website:

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- The school web site complies with statutory DFE requirements
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website
- Policies are available in print upon request

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

Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Prevent

St Gerard's has a duty to protect our pupils from accessing terrorist and extremist material on the Internet. The School will therefore aim to do the following:

- Educate pupils on the appropriate use of social media and the dangers of downloading and sharing inappropriate material including that, which is illegal under the Counter- Terrorism Act.
- Ensure that pupils are unable to access any inappropriate Internet sites whilst using the school computers/ laptops through the use of appropriate filtering, firewalls and security settings.
- Educate pupils through lessons and assemblies on the concepts of Radicalisation and extreme ideology.
- Inform pupils on the importance of Internet Safety both through the Computing curriculum and PHSE education.

Agreed by Governing Body:
Date of next Review: October 2018: