Excellence together with Christ at the Centre

St. Anne's and Guardian Angels Catholic Primary School

Excellence together with Christ at the centre

St Anne's and Guardian Angels

E-Safety Policy	
Updated by Natalie Chapple	September 2021
Date to be reviewed	September 2021

St Anne's and Guardian Angels vision is:

"For everyone to achieve to their full potential in a safe, happy and supportive environment."

- To support every child in achieving their best through high quality teaching of a rich curriculum with Catholic values at the core.
- To nurture well rounded and happy children ready for the next stage in their life.
- For results to be at least in line with national expectations
- For staff to have a good understanding of children's social, emotional and spiritual needs and how to respond appropriately to these
- For parents and parish to play an active role in the school community
- To have a stable staff with a high quality of staff wellbeing as a foundation for the continued development of the school.

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 students 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 Head-teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student 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.
- Unauthorized 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 students' / 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.

Scope of the Policy

- This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
- The Education and Inspections Act 2006 empowers Head-teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
- The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students 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.
E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT / PSHCE / 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 such as the detrimental effect of cyber-bullying should be reinforced as part of a planned programme of assemblies and activities.
- Students 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.
- Students should be helped to understand the need for the student AUP (Acceptable Use Policy) and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- 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 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 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).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, texts, newsletters, website, school blogs.
- Parents workshops.
- Reference to the outside agencies.

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 will identify e-safety as a training need within the performance management process.
- 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 Officer will receive regular updates through attendance at LA training sessions and by reviewing guidance documents released by BECTA / LGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Officer will provide advice / guidance / training as required to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee 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 / LGfL or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The school in liaison with **Turn IT On** (ICT Support Company) 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 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 in the Acceptable Usage Policy and 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.
- The "administrator" passwords for the school ICT system, used by the Network Manager (ICT Technician) must also be available to the Head-teacher or ICT Subject Leader and kept in a secure place (e.g. 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 Exa Surfprotect.

- In the event of the Network Manager (or ICT Subject Leader) 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 Head-teacher.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and ICT Subject Leader. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.
- 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.
- An appropriate system is in place for users to report any actual / potential e-safety incident to the ICT Subject Leader and a member of the senior leadership team.
- Appropriate security measures are in place (i.e. scanning of external devices before opening using Sophos) 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 is in place for temporary access of "guests" (e.g. trainee teachers, visitors - See Staff and Volunteer Acceptable Use Policy for further detail) onto the school system.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on laptops and other portable devices that may be used out of school. (see School Personal Data Policy in the for further detail)
- An agreed policy is in place (i.e. only the ICT Subject Leader and IT Technician have administration rights) that allows staff to / forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

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. This should be done every time any form of ICT is used in class.

- 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 students are allowed to search the internet it will be by using specified search engines eg. Google Safe Search or Ask Kids, 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 (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (or ICT Subject Leader) 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.
- Students should be taught in all subject lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect

copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' 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 are published on the school website and the school's social media platforms.

SAFE USE OF IMAGES CONSENT FORM

In School, images (photographs, videos etc.) are often taken of the children doing a range of activities and the children use electronic equipment such as digital cameras and iPads as part of their work. These images may be used in our school prospectus, in other printed publications, on our school website, social media sites, class blogs, or on project display boards in school. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use. Occasionally our school may be visited by the media who will take photographs or film footage of a high profile event, or to celebrate a particular achievement. Pupils might appear in these images, which may appear in local or national newspapers or in televised programmes. (See Conditions of Use attached to this form for more information on use of images by the media). The School believes that the taking and use of photos and videos is usually a very positive experience for those involved and that all pupils are to be included unless parents/carers have specifically opted them out. The aim of the School is therefore to have a reasonable, practical approach to the taking and use of photographic images of children and to honour our obligation of a duty of care to all pupils. The welfare and safety of the children will always be uppermost in the School's decision making and the School will ensure there is proper regard to the law and the protection of vulnerable individuals. The

School requires your permission for images to be taken of your child and used, as described, during the 2018/2019 academic year.

CONDITIONS OF USE Parents/legal carers must note that once an image is made available outside of the School environment (e.g. on the internet), it can remain on that type of media technology forever. In addition, a parent/legal carer's future retraction of their consent to images being used does not mean the image(s) can be removed.

- The school will not use the personal details or full names (which means first name and surname) of any child or adult in a photographic image, on video, on our website, social media and blogging sites, in the school prospectus or in any of our other printed publications.
- We may include pictures of pupils and teachers that have been drawn by pupils. We may use group or class photographs or footage with very general labels, such as 'a science lesson'.
- We will only use images of pupils who are suitably dressed.
- Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.
- Safe use of Images Consent forms will be updated at the beginning of each academic year.
- If you want your child's image removed from the website, social media pages and other school documentation, you must inform the office in writing.

Notes on Use of Images by the Media

If you give permission for a child's image to be used by the media then you should be aware that:

• They may wish to publish the child's name, age and the school name in the caption for the picture, you would be informed of this and extra consent obtained, (possible exceptions to this are large group or team photographs);

• It is possible that the newspaper will re-publish the story on their website, or distribute it more widely to other newspapers or media organisations.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

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

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

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.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device once it has been transferred or its use is complete.

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				Students / 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	*						*	
Use of mobile phones in lessons				*				*
Use of mobile phones in social time		*						*
Taking photos on personal mobile phones or other				*				*
Use of hand held devices eg iPads		*						*
Use of personal email addresses in school, or on		*						*
Use of school email for personal emails				*				*
Use of chat rooms / facilities				*				*
Use of instant messaging				*				*
Use of social networking sites				*				*

Use of blogs		*				*		

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 students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – 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 students or parents / carers (email, chat, blog posts /comments etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students 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.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

St. Anne's and Guardian Angels Catholic Primary School

Excellence together with Christ at the Centre

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse					*
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud					*
	adult material that potentially breaches the Obscene Publications Act in the UK					*
	criminally racist material in UK					*
	pornography					*
	promotion of any kind of discrimination				*	
	promotion of racial or religious hatred					*
	threatening behaviour, including promotion of				*	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				*	
Using school systems to run a private business					*	

Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LGfL and / or the school		*			

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more 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 normal behaviour / disciplinary procedures.

Natalie Chapple IT lead

Date September 2021
Renewal September 2023