



The Federation of St Elphege's and Regina Coeli Catholic Schools



Internet Safety Policy

Scope:	Federation	
Date Adopted:	October 2009	
This Review:	December 2019	
Next Review:	Autumn Term 2020	Health, Safety and Welfare
Approved:	November 2018	Annually, or when regulations change



Internet Safety Policy



The Federation of St Elphege's and Regina Coeli Catholic Schools



'With God all things are possible'

'Where there is love, there is God'

With the help of God's love, the Federation of St Elphege's and Regina Coeli Catholic Schools will seek to develop the whole child. Each child is uniquely created and precious to God and it is the Federation's mission, guided by the Holy Spirit, to nurture each child's spiritual, moral and academic growth.

Inspired by the teachings of Christ we will...

- Develop our children's faith, spirituality and joy in the love of God
- Educate our children to the highest standards thus realising their own potential
- Instil in our children the knowledge, skills and confidence to succeed and take pride in their achievements recognising we each have special gifts and talents
- Encourage everyone to be more than they thought possible, in a secure and loving environment
- Promote a caring community where we will all behave well. We will be dignified in our actions, demonstrating good manners, tolerance, kindness and generosity to ourselves and others
- Prepare our children today to become tomorrow's responsible and independent individuals equipped to face life's challenges
- Ensure our Federation is a happy, safe and welcoming place where we all enjoy learning, work hard, support one another and do our best
- Create an active partnership of love, joy and high expectations between children, parents, carers, staff, governors, parishes and the wider community

Inclusion statement

The school community will ensure that ALL children irrespective of race, ethnicity, nationality, gender (including those who identify as transgender), sexual orientation, ability, special educational need, disability, faith or religion, age, culture, socio-economic or home background will have equal access to the breadth of this curriculum.

The achievements, attitudes and well-being of all our children matter and the school will endeavour to promote their individuality. Children with learning disabilities and gifted and talented children will be allowed to express themselves according to their ability. Work will be differentiated to meet their needs and achievements will be celebrated.

This Policy will be implemented through on going consultation with all members of the school community.

Internet Safety Policy

The Federation of St Elphege's and Regina Coeli Catholic Schools

The Federation's Internet Safety Policy relates to the suite of Safeguarding Policies as well as the Computing Policy, Positive Behaviour Policy, PSHE (including Citizenship) Policy, the Home-School Agreement, Staff- School Devices: Acceptable User Statement, Mobile Phone Policy, Data Protection Policy and Data Retention Policy.

The Internet Safety Policy will be reviewed on a yearly basis. It will be agreed by senior management and approved by governors.

ICT has an all-encompassing role within the lives of children and adults. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- Email
- Instant messaging
- Video messaging / calling
- Blogs
- Podcasting
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download services
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones and tablets

This policy applies to all members of The Federation of St Elphege's and Regina Coeli Catholic Schools' community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Federation's computing systems, both within and outside of the school setting.

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 online bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Anti-Bullying Policy or Positive Behaviour Policy.

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 online safety behaviour that take place out of school.

Why is Internet access important?

The purpose of internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Access to the internet is a necessary tool for staff and students. It is an entitlement for staff and students who show a safe, responsible and mature approach to its usage.

What are the dangers?

The use of such technology greatly enhances communication and the sharing of information and at The Federation of St Elphege's and Regina Coeli Catholic Schools, pupils and staff are to be encouraged to use technology in a positive and responsible way. However, the use of technology can put young people at risk within and outside of school. Some of these dangers include but are not limited to:

- Access to illegal, harmful or inappropriate images or other content.
- Exposure to extremist or radical views
- Unauthorised access to / loss of/ sharing of personal information.
- The risk of being subject to grooming by those with whom children 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. (See Positive Behaviour Policy)
- Access to unsuitable images / video / 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.

Children of primary school age should not have access to social networking sites, such as: Facebook, Instagram, Snapchat, Whatsapp. Children using these services are in danger of exposure to explicit, dangerous or inappropriate material.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This policy document has been drawn up to protect all parties – the students, the staff and the school - and aims to provide clear advice and guidance on how to minimise risks.

What are the benefits to the school?

A number of studies and government projects have indicated the benefits to be gained through the appropriate use of the internet in education.

These benefits include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in government initiatives such as NGfL ,Virtual Teacher Centre, MLE
- Information and cultural exchanges between students world-wide;
- Educational, cultural, vocational, social and leisure use in libraries, clubs and at home;
- Discussion with experts in many fields for pupils and staff;
- Staff professional development - access to educational materials and good curriculum practice;
- Communication with the advisory and support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LEA, DfE, Ofsted and parents.

How will Internet use provide effective learning?

Teachers, parents and pupils need to develop good practice in using the internet as a tool for teaching and learning. There is a fine balance between encouraging autonomous learning and maintaining adequate supervision. Systems to ensure internet use is as safe as possible will enable increased use and the quality of that use becomes a critical factor.

- Internet access is provided by the London Grid for Learning. It provides a service designed for pupils. This includes filtering appropriate to the age of all pupils in London. It is monitored and maintained by the school's preferred contractor, Cygnet IT Services.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirement for staff and pupils. Staff will work within the guidelines of the Staff- School Devices: Acceptable User Statement.
- Pupils will be given clear objectives for internet use through the computing curriculum and the Home-School Agreement.
- Sites will be selected which will support the learning outcomes planned for pupils' age and maturity;
- Pupils will be educated in taking responsibility for Internet access regularly in partnership with recognised bodies such as Childnet and CEOP. Pupils across the school will be trained as E-buddies to support their peers and develop e-Safety alongside the School Parliament and the PHSE and Citizenship curriculum.

How will pupils be taught to assess Internet content?

Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher. This level of control is not so straightforward with Internet-based materials. Therefore, computing teaching should be widened to incorporate an element of digital literacy including the ability to discern the reliability of internet media, for instance the value and credibility of web materials in relationship to other media. The tendency to use the web when better information may be obtained from books may need to be challenged.

- Pupils will be taught ways to validate information before accepting that it is necessarily accurate;
- Pupils will be taught to acknowledge the source of information, when using internet material for their own use;
- Pupils will be made aware that the writer of an email or the author of a Web page might not be the person claimed;
- Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

How will email be managed?

Email is an essential means of communication within education. Once email is available it is difficult to control its content. Nevertheless, children's school email content should not be considered private. Staff email accounts will be private unless there is a valid reason for the system's administrator to monitor the content of the account. Individual email accounts are automatically set up through SIMS when a child enters the school, but are only distributed to pupils in Year 1, when the curriculum demands. Whole-class email accounts are also set up for each class in the schools, the choirs, 3 school email accounts, and for other stakeholders where a need arises. All members of staff are given access to their account when they join the school. Staff and Pupil email accounts are removed or transferred on leaving the school.

- Pupils need to use email as part of the curriculum and in development of their computing skills.
- Email must only be used for valid, educational purposes.
- Pupils and staff can gain access to school email from any internet access point.
- From Year 1, pupils will be given individual email accounts with their own password. This assumes a high level of trust and all pupils and parents are asked to sign the Home-School Agreement. Teachers have access to their pupils' email addresses and passwords. The designated systems administrators have access to ALL email addresses and passwords and have the access to create or close email accounts.
- In-coming and out going e-mail is monitored by LGfL for content and filtered where necessary. Where any staff or pupil account is misused, it is identified and suspended or closed. Serious misuse can result in an investigation and police action, ie. under safeguarding or privacy issues.
- Messages sent using the school domain name should be regarded in the same way as messages written on school headed paper;
- The forwarding of chain letters is forbidden and social networking sites can not be accessed from any school computers, without appropriate permissions, due to the filtering systems provided by LGfL.

NB: Governor Services and staff communication with the governing body will only use LGfL mail providers to communicate any information that is considered sensitive. Even when communicating through LGfL mail providers, confidential information will be encrypted.

How will publishing on the Web be managed?

The School web site will become a source of stand alone information for a wide audience. It will reflect the schools' ethos and provide information that is accurate and up to date, incorporating the school's prospectus and relevant information to prospective parents and other bodies.

As the school's web site can be accessed by anyone on the internet, the security of staff and pupils is vital. Photographs and videos which identify individuals will not be used unless consent has been obtained from a parent or carer. While any risks might be small, the parents' perception of risk must also be taken into account

The development of the schools' website will enable pupils and staff to publish work, photographs and videos to create a global public image of the school.

- The head teacher will delegate editorial responsibility to a member of staff to ensure that content is accurate and quality of presentation is maintained. This will likely include the Computing Coordinator, and other key members of staff.
- All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name.
- The point of contact on the web site should be the school address and telephone number. Home information or individual email identities will not be published.
- Consent from parents will be sought before photographs or videos of pupils are published digitally such as media use in newspapers, CDs following school journeys, Year 6 Yearbook, DVDs of school performances being distributed to parents etc. *See Data Protection Policy for more information.*
- The Head teacher takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to our website authorisers.
- The school website complies with the school's guidelines for publications.
- Photographs published on the web do not have full names attached, unless explicit consent is obtained.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Use of Digital and Video Images

Where necessary, consent will be obtained from parents or carers prior to a pupil featuring in digital media. Parents and carers have the right to withdraw this consent at any time. *See Data Protection Policy.*

Examples of how digital photography and video may be used within school include:

- Pupils being photographed (by the classroom teacher, teaching assistant or another pupil) as part of a learning activity e.g. photographing pupils at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the pupils to see their work and make improvements.
- A pupil's image for presentation purposes around the school e.g. in school wall displays and PowerPoint presentations to capture images around the school or in the local area as part of a project or lesson.
- A pupil's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators e.g. on a portable storage device or a document sharing good practice; in our school prospectus or on our school website. If images or videos taken whilst on the school site are to be used for purposes outside of the Federation or to be published on the internet, consent will be obtained from parents / carers. Unfortunately, whilst adequate care will be taken by school staff to avoid scenarios where third parties obtain images of children whilst in the public domain, for example on a school trip, the school cannot be held responsible for how these images are used by third parties.
- On rare occasions, a pupil's image could appear in the media if a newspaper photographer or television film crew attend an event. If these images are taken on the school site, the school will ensure that it holds the relevant consent from parents and carers before any images are taken. However, if these images are taken in the public domain, for example on a school trip, whilst every care will be taken by the school to respect the parents / carers wishes regarding the publication of images, the school cannot be held responsible for how these images are used by third parties.

Note: If a circumstance arose where the school wanted to link a pupil's image to their name e.g. if the pupil won a national competition and wanted to be named in local or government literature, parents would be contacted explicitly for permission.

The following safeguarding principles are followed with specific regard to the use of digital and video images:

- The school gains parental / carer permission for use of digital photographs or video involving their child on entry to the school. Parents and carers may withdraw this consent at any time. *See Data Protection Policy.*
- Only images of pupils in suitable dress are used.
- Parents volunteering on class trips are not allowed to take photographs or videos on their personal equipment.
- Digital images /video of pupils will only be stored on secure school owned systems or devices and only retained for the period that consent remains and they are necessary.
- The school does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs without the explicit consent of the parent / carer.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils. Staff and pupils are also required to adhere to the Federation's Mobile Phone Policy.
- The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their eSafety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file or geotagging data), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

CCTV

CCTV is used in some areas across the Federation's sites as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained by the Support Provider for 28 days), without permission except where disclosed to the Police as part of a criminal investigation.

What other Internet applications are available?

The internet is a rapidly developing resource with a wide range of web-based applications available to the end user. These applications have the potential to offer benefits to the administrative tasks schools staff and teachers are required to carry out and also offer the potential for a broader and more relevant and balanced curriculum experience for children. Any web-based application and any instances of cloud computing used within the school will have associated data protection and integrity risks assessed to ensure that they meet UK Education guidelines, prior to any data being uploaded. Applications which offer the ability to communicate, including conferencing applications such as Chat, Social networking, Newsgroups and Webcams will also be subject to the same rigorous risk of data security assessment. Many of these facilities have great potential for education, for instance pupils could exchange live text, speech or video with a similar class in South Africa or Italy, at low or zero cost. A non-exhaustive list of the considerations new web-based applications will be subject to is listed below:

- Pupils will not be allowed to access public chat rooms. LGfL filters all social networking sites and primary school age children are under age for their use, reflecting the need for greater maturity before this area of the internet is given free access.
- Newsgroups are only available to pupils through the use of an approved internet schools package, Espresso, where the content is age appropriate.
- New facilities will be thoroughly tested and any legal or safeguarding implications considered carefully before pupils are given access.

How will Internet access be authorised?

Access to the Internet in school is on the basis of educational need. All staff and children have internet access through the NGfL which is managed by Cygnet IT Services. This is a well managed and securely filtered intranet which enables pupils and staff to use and search the internet safely and securely. There is a robust system in place to notify Cygnet of any breaches of security to enable sites to be blocked immediately.

- Internet access is a necessary part of the statutory curriculum. It is an entitlement for pupils based on responsible use;
- Through all phases, Internet access will be granted to a whole class or to individuals as part of the scheme of work, with suitable education in responsible Internet use as part of Computing, PHSE, Citizenship, Anti Bullying and Safeguarding.
- Staff must comply with the Staff- School Devices: Acceptable User Statement which must be countersigned by a member of the Senior Leadership Team (SLT)

How will the risks be assessed?

It is difficult to remove completely the risk that pupils might access unsuitable materials via the school network. In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. The school cannot accept liability for the material accessed, or any consequences thereof.

- The use of computer systems / computing devices without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990;
- Staff laptops taken off-site which contain sensitive data will have password protected encryption to ensure that sensitive pupil data is secure. Where the laptop itself does not contain sensitive data, encryption will not be necessary. However, staff members must use encrypted storage devices when working on terminals (which are not themselves encrypted) outside of the school sites.
- Methods to identify, assess and minimise risks will be continually reviewed.
- Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken and should any material be deemed unsuitable the material will be removed from the terminal and it will be reported immediately to Cygnet for blocking.
- The Head teacher will ensure that the policy is implemented effectively.

How will the school ensure Internet access is safe?

The Internet is a communications medium that is freely available to any person wishing to send messages, transfer data / media or publish information on almost any topic. Access to appropriate information should be encouraged and Internet access must be safe for all members of the school community from youngest pupil to teacher and administrative officer. Pupils and staff will have appropriate protected access to the internet.

The technical strategies being developed to restrict access to inappropriate material fall into several overlapping types (sometimes all referred to as filtering)

The main systems used are :

- Blocking strategies remove access to a list of unsuitable sites or newsgroups. Maintenance of the blocking list is a major task as new sites appear every day and is managed by Cygnet, NGfL and Atomwide.
- Filtering examines the content of Web pages or e-mail messages for unsuitable words. Filtering of Web searches attempts to block a current loophole.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.

None of these systems can be completely effective and a combination of approaches will be required, alongside adequate supervision.

- Blocking and/or filtering is performed by NGfL, Atomwide and Cygnet where a wide area network is used. The security of the school ICT systems will be maintained in close liaison with Cygnet and the LGfL. At school-level network safeguarding is carried out by a Cygnet technician for all devices which access the internet.
- Virus protection will be installed and updated regularly.
- The Cygnet technician will ensure that the system has the capacity to take increased traffic caused by internet use.
- Personal USB storage devices may not be brought into school without specific permission and a virus check. Staff working with pupil data will use secure USB devices to protect sensitive data.
- Pupils will be informed that Internet use will be supervised and monitored;
- The school will work in partnership with parents, LGfL, the DfE and Cygnet to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to the Cygnet via the Computing co-ordinator or a member of the SLT.
- Any material that the school suspects is illegal will be referred to the Internet Watch Foundation.
- Where minority languages are involved, appropriate measures will be used to ensure the process to select appropriate material is adequate.

How will complaints regarding internet use be handled?

Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the issue has arisen through internet use inside or outside school. Transgressions of the rules could include minor as well as the potentially serious and a range of sanctions are required, linked to the school's Behaviour, PHSE, Citizenship, Whistleblowing and Safeguarding policies.

- Responsibility for handling incidents will be given to senior members of staff.
- Pupils, parents and staff will be informed of the complaints procedures.
- Parents and pupils will need to work in partnership with staff to resolve issues
- There may be occasions when the LA and/or police must be contacted. Early contact will be made to establish the legal position and discuss strategies.
- Staff members or pupils may have email or internet access denied depending on the nature of the incident;

Complaints regarding the internet may also be managed under the Federation's Complaints Policy.

How will staff and pupils be consulted?

It is important that staff feel prepared to teach about the safe and responsible use of the internet and that they personally subscribe to the school Internet Safety Policy. Staff will be given opportunities to discuss the issues and develop appropriate teaching strategies, with training where necessary.

- Rules for Internet Safety will be posted near computer systems. All children and staff will be required to sign the Home-School Agreement.
- All staff including teachers, supply staff and teaching assistants will be provided with the Internet Safety Policy, and its importance explained.
- Parents' attention will be drawn to the policy in newsletters, the school brochure and on the school website.
- A module on responsible Internet use will be included in the Computing and PSHE+C Curriculum and detailed during Anti-Bullying week programme covering both school and home use.
- Safe and responsible internet use is an ever-apparent theme across the Federation's Computing Curriculum.

How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the internet. Through the distribution of carefully selected resources and a series of e-Safety workshops, parents will be taught how best to promote internet safety at home.

- A careful balance between informing and alarming parents will be maintained.
- Demonstrations and practical workshops for parents will be organised to encourage a partnership approach
- Joint home / school guidelines on issues such as safe Internet use will be established.
- A list of relevant information from organisations such as BECTa, Childnet and CEOP will be maintained.

How is Internet used across the community?

Internet use in the local community is becoming common. In addition to the home, access is available at the local library and after school clubs etc. Each organisation has its own approach and pupils may find variations in the rules and even unrestricted access to the internet. Although policies may differ in detail, community partners adhere to the same laws as schools with respect to content, copyright and misuse.

- In libraries, parents/carers of children under 18 years of age will generally be required to sign an acceptable use policy on behalf of the child;
- In libraries, adult users will also need to sign the acceptable use policy;
- In libraries, children under 8 years of age must be accompanied by an adult when accessing the internet, due to the Children's Act.
- Rules for internet access will be posted near computer systems, or will be available on request. Rules are there to protect legitimate use.
- Suitable educational, vocational and leisure use is encouraged in community facilities.

Roles and Responsibilities

This policy applies to all pupils, parents and carers, teaching and support staff, governors, volunteers, students and visitors. This list is not to be considered exhaustive.

The Role of Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/ mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parent evenings, newsletters, letters, website, e-safety campaigns or literature. Parent/ carers should understand the contents of this policy and sign the Home-School Agreement.

The Role of Teaching and Support Staff

- To have an up-to-date awareness of e-safety matters and of the current school policy and practices related to e-safety.
- To report any suspected misuse or problem to the Designated Person/s for Child Protection for investigation/ action/ sanction.
- To ensure any digital communications with pupils are minimal, necessary and on a professional level and only carried out using the official school systems.
- To ensure personal information including telephone contact details, personal email addresses and addresses, are not provided to pupils.
- To carry out the school's E-safety programme of work and embed in everyday practice in all aspects of the curriculum.
- To ensure pupils understand and follow the e-safety rules.
- To ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- To monitor ICT activity in lessons and extra-curricular/ extended school activities as appropriate.
- To be aware of e-safety issues related to the use of mobile phones, cameras, smart watches and other hand held devices which should not be within the children's possession in school.
- To ensure that in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with unsuitable material that is found in Internet searches.
- To understand the contents of this policy and other e-safety related policies and to sign the Staff AUP

The Role of the Designated Person/s for Child Protection

- To provide support and advice to staff as regards potential e-safety issues.
- To liaise with the Computing Subject Leader and other staff in regards to the implementation and monitoring of the e-safety programme of work.
- To update the head teacher and Governors of any e-safety issues that require attention.
- To be aware of the Prevent Duty (Radicalisation and Extremism), how to make a Channel Referral and to ensure that there is adequate training for staff on the Prevent Duty. See Safeguarding Policy.
- To attend training in e-safety issues and be aware of the potential for serious child protection issues to arise from:
 - Sharing of personal data.
 - Access to illegal/ inappropriate materials.
 - Inappropriate on-line contact with adults/ strangers.
 - Potential or actual incidents of grooming.
 - Cyber-bullying.

The Role of Pupils

- To abide by the school's rules for safe Internet Use.
- To avoid plagiarism and uphold copyright regulations.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- To abide by the school's policy as regards the use of mobile phones, cameras and other digital devices.
- To understand and abide by the school's anti-bullying policy.
- To understand the importance of adopting good e-safety practices outside of school.

Data security: Management Information System access and Data transfer

Strategic and Operational Practices

At this school:

- We have appointed a DPO and we ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in Single Central Record.
- Any person using school owned computer systems will be required to sign and understand the relevant Acceptable Usage Policy. This makes clear the responsibilities of all persons with regard to data security, passwords and access.
- We follow LA/DfE/Safeguarding guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We follow all requirements under the General Data Protection Legislation (GDPR) and the latest data protection legislation in England.
- We require that any sensitive material must be encrypted if the material is to be removed from the school and limit such data removal. We have an approved remote access solution so that certain nominated staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access are working within the approved system and follow the security processes required by those systems.

Technical Solutions

- Staff have a secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems or lock their account when leaving their computer.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content
- We store sensitive, unencrypted materials in lockable storage cabinets or in private and secure areas of the school.
- All servers are in lockable locations and managed by DBS-checked staff.
- We comply with legislation by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been stored.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is collected by secure data disposal service.



**The Federation of St Elphege's
and Regina Coeli Catholic Schools**



Children's Charter for Responsible Network, Internet and Mobile Phone Use

The school has provided computers, tablets, cameras and internet access to help children's learning. Many children also use mobile phones to communicate with children who attend this and other schools. These rules will keep everyone safe and help us be fair to others.

- I will ask permission from a member of staff before using the internet or my mobile phone in school.
- I will use only my own username and password for my LondonMail email, Mathletics, Class DoJo and any other school accounts I have. I will keep my passwords secret.
- I will not use another person's username and password to access their online accounts and I will not use anyone's phone without permission.
- I will not access or delete other people's files on the school network.
- I will not bring CDs or USB storage devices into school unless I have permission.
- I will only email / message people I know or people my teacher has approved.
- The messages I send online / via text message or messaging app will be polite and sensible.
- I will not give my full name, address or phone number to anyone online.
- I will not post photos or videos of myself or others online unless my teacher, parent or carer has approved.
- I will not access games, videos, websites or pictures which I think might be inappropriate for my age.
- I will not arrange to meet anyone online unless I know them in real life and my parent or carer has said that I am allowed to.
- To help protect other pupils and myself, I will tell an adult I trust if I see anything I am unhappy with or I receive messages I do not like.
- I understand that the school may check my computer files and messages on school accounts.
- I understand that the school may monitor the internet sites I visit.

(Please detach this section for your records and return the reply slip below to your child's class teacher)

<p>Parent / Carer Child's Name: Class: I have read and discussed the Children's Charter for Responsible Network, Internet and Mobile Phone Use with my child and agree to support the school and my child in upholding each of the statements. Date: Signed:</p>	<p>Child (Year 1 – Year 6) I understand that I must behave in a sensible and responsible way online and when I am using a mobile phone. I understand that I must keep personal information private and talk to an adult I trust if anything makes me worried or upsets me. Child Signed:</p>
--	---

The ethos of The Federation is founded on the Gospel values proclaimed by Christ. Through our teaching and learning, we aim to reaffirm these values and, in so doing, portray God's loving presence in all our lives.

Our aims and objectives for behaviour and the curriculum, are inspired by the Gospel teachings of Jesus. It is with the strength of the Holy Spirit and God the Father's love for us that we achieve these aims.

The unique contribution that every child makes to the life of the schools is greatly valued. Each child is encouraged to achieve their best, according to their talents, interest, age and ability.



The Federation of St. Elphege's Catholic Schools
 Millison Drive
 Surrey
 SM6 5HY
 Telephone: 020 8688 5306
 www.stelphageschools.org.uk
 info@stelphageschools.org.uk

Regina Coeli Catholic Primary School
 173 Pangplford Road
 South Croydon
 CR2 6DF
 Telephone: 020 8688 4582
 www.reginacoeliscatholic.co.uk
 office@reginacoeliscatholic.co.uk

At The Federation of St Elphege's and Regina Coeli Catholic Schools, we provide a secure environment in which all children and adults can learn and work together.



This is a happy and caring community which enables everyone to achieve their best.

Home-School Agreement

The Federation of St Elphege's and Regina Coeli Catholic Schools



Child's Name

Child's Class

2019 - 2020

*With God all things are possible
 Where there is love there is God*

The Federation Will:

- Provide a safe and secure environment in which all children and adults can learn and work together.
- Teach tolerance and respect for all to provide a happy and caring community to enable everyone to achieve their best.
- Encourage children to value others and take care of their surroundings.
- Let parents know about any concerns or problems that affect their child's work, behaviour or attendance.
- Inform parents of their child's progress through annual written reports, regular meetings and informal discussions with the class teacher.
- Set regular homework in line with The Federation's English and Maths policy.
- Keep parents informed about school activities through regular newsletters.

Signed on behalf of

The Federation of St Elphege's and Regina Coeli Catholic Schools

Signed:

Date:

As a Parent or Carer I will:

- Make sure my child attends school every day and notify the school when my child is absent by 'phoning on the first day of absence.
- Make sure that my child arrives on time with everything that is needed.
- Ensure my child wears the correct uniform, clearly labelled with their name.
- Ensure appropriate behaviour and internet safety by supporting and reinforcing the school's policy and guidelines for internet safety.
- Support my child with homework.
- Attend Parents' Consultation meetings, workshops and discussions to support my child's progress.
- Treat all members of the school community with courtesy and respect.
- Respect the privacy and rights of all members of the school community by refraining from sharing information or photographs on the internet and social media networks.
- Inform the school in writing if my child's dietary or medical needs have changed and, where appropriate, provide the necessary medication with signed consent to administer it.

Parent or Carer's Signature

Signed:

Date:

As a Pupil I Will:

- Treat others as I would like to be treated.**
- Behave sensibly at all times.**
- Always tell the truth.**
- Listen, work hard and always do my best.**
- Always be kind, gentle and polite.**
- Care for myself, others, our property and environment.**
- Speak to an adult I trust if something upsets or worries me.**
- Make sure that an adult knows where I am at all times.**

Follow the Children's Charter for Responsible Network, Internet and Mobile Phone Use.

Child's Signature

Signed:

Date:



The Federation of St Elphege's and Regina Coeli Catholic Schools



Acceptable Internet & School Network / Device User Statement

For Staff

IT systems used by the school are licenced to / owned by the school and are made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Acceptable Internet & School Network / Device User Statement has been drawn up to protect all parties - the pupils, the staff and the school.

The Designated Safeguarding Officers are **Martin Jones & Tessa Christoforou**.

The school reserves the right to examine or delete any files that may be held on its local and externally licenced networks to monitor any Internet sites visited.

- Access must only be made to authorised accounts, for which account details and passwords must not be made available to any other person.
- All Internet use should be appropriate to staff professional activity or pupil's education.
- It is strongly recommended that all staff using social networking sites at home maintain strong security settings to protect their integrity and professionalism and that of the school. Activity that can be interpreted as internet bullying or bringing the school into disrepute will not be tolerated and disciplinary and/or legal action may be taken against parties involved.
- Activity that threatens the integrity of the school or IT systems, or that attacks or corrupts other systems, is forbidden; disciplinary and/or legal action may be taken against parties involved. This includes the intentional or unintentional installation of malicious, illegal or inappropriate software or files.
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should report unsuitable sites and materials to the Designated Safeguarding Officers. Use of inappropriate sites or materials on school owned laptops is forbidden and will result in the laptop being removed from use; disciplinary and/or legal action may be taken against parties involved.
- Users are responsible for all correspondence made using school owned accounts. Email content is monitored through the Cygnet and LGfL Web filtering system.

- The same professional levels of language and content should be applied as for letters or other media, particularly as internet correspondence is often forwarded. Malicious internet correspondence (including social networking) will not be tolerated and may result in restricted account access, disciplinary and/or legal action.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Copyright of materials and intellectual property rights must be respected.
- Legitimate private interests may be followed, providing school use and face-to-face teaching is not compromised.
- Images of pupils and/ or staff will only be taken, stored and used for educational purposes in-line with schools e-safety policy. Publishing or sending media through IT systems which are external to the school containing identifiable information relating to pupils or staff will be solely with the express permission of parents/carers, the SLT and in-line with the Federation's Internet Safety Policy.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I understand that data and files created explicitly or generated implicitly as part of background processes whilst using school owned IT equipment may be stored on Federation owned IT equipment and therefore remains the property of the Federation of St Elphege's and Regina Coeli Catholic Schools. The school cannot be held responsible for the data security of any personally generated information that it is not explicitly made aware of.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Any data stored on Federation owned devices, systems or cloud services should be considered the property of The Federation of St Elphege's and Regina Coeli Catholic Schools.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Director of Finance and Operations for approval.

Full Name: _____

Position: _____

Signed: _____

Date: _____

Appendix 4: e-Safety Resources

All school stakeholders, including children and parents, are encouraged to visit the London Grid for Learning's online safety pages. Technology advances are rapid and therefore resources which are included in any policy are likely to become 'out-of-date' quickly. LGfL collate and maintain trusted and current resources for promoting children and young people's online safety. Please click the image below or follow this URL:

<https://www.lgfl.net/online-safety/resource-centre?a=1>



E-safety in Key Stage 1

Knowledge & understanding	Skills
<ul style="list-style-type: none"> Can they understand the different methods of communication (e.g. email, online forums etc)? Do they know you should only open email from a known source? Do they know the difference between email and communication systems such as blogs and wikis? Do they know that websites sometimes include pop-ups that take them away from the main site? Do they know that bookmarking is a way to find safe sites again quickly? Can they begin to evaluate websites and know that everything on the internet is not true? Do they know that it is not always possible to copy some text and pictures from the internet? Do they know that personal information should not be shared online? Do they know they must tell a trusted adult immediately if anyone tries to meet them via the internet? 	<ul style="list-style-type: none"> Can they follow the school's safer internet rules? Can they use the search engines agreed by the school? Can they act if they find something inappropriate online or something they are unsure of (including identifying people who can help; minimising screen; online reporting using school system etc)? Can they use the internet for learning and communicating with others, making choices when navigating through sites? Can they send and receive email as a class? Can they recognise advertising on websites and learn to ignore it? Can they use a password to access the secure network?

E-safety in Years 3 and 4

Knowledge & understanding	Skills
<ul style="list-style-type: none"> Do they understand the need for rules to keep them safe when exchanging learning and ideas online? Can they recognise that information on the internet may not be accurate or reliable and may be used for bias, manipulation or persuasion? Do they understand that the internet contains fact, fiction and opinion and begin to distinguish between them? Can they use strategies to verify information, e.g. cross-checking? Do they understand the need for caution when using an internet search for images and what to do if they find an unsuitable image? Do they understand that copyright exists on most digital images, video and recorded music? Do they understand the need to keep personal information and passwords private? Do they understand that if they make personal information available online it may be seen and used by others? Do they know how to respond if asked for personal information or feel unsafe about content of a message? Can they recognise that cyber bullying is unacceptable and will be sanctioned in line with the school's policy? Do they know how to report an incident of cyber bullying? Do they know the difference between online communication tools used in school and those used at home? Do they understand the need to develop an alias for some public online use? Do they understand that the outcome of internet searches at home may be different than at school? 	<ul style="list-style-type: none"> Do they follow the school's safer internet rules? Do they recognise the difference between the work of others which has been copied (plagiarism) and re-structuring and re-presenting materials in ways which are unique and new? Can they begin to identify when emails should not be opened and when an attachment may not be safe? Can they explain how to use email safely? Can they use different search engines?

E-safety in Years 5 and 6

Knowledge & understanding	Skills
<ul style="list-style-type: none"> • Can they discuss the positive and negative impact of the use of ICT in their own lives and those of their peers and family? • Do they understand the potential risk of providing personal information online? • Do they recognise why people may publish content that is not accurate and understand the need to be critical evaluators of content? • Do they understand that some websites and/or pop-ups have commercial interests that may affect the way the information is presented? • Do they recognise the potential risks of using internet communication tools and understand how to minimise those risks (including scams and phishing)? • Do they understand that some material on the internet is copyrighted and may not be copied or downloaded? • Do they understand that some messages may be malicious and know how to deal with this? • Do they understand that online environments have security settings, which can be altered, to protect the user? • Do they understand the benefits of developing a 'nickname' for online use? • Do they understand that some malicious adults may use various techniques to make contact and elicit personal information? • Do they know that it is unsafe to arrange to meet unknown people online? • Do they know how to report any suspicions? • Do they understand they should not publish other people's pictures or tag them on the internet without permission? • Do they know that content put online is extremely difficult to remove? • Do they know what to do if they discover something malicious or inappropriate? 	<ul style="list-style-type: none"> • Do they follow the school's safer internet rules? • Can they make safe choices about use of technology? • Do they use technology in ways which minimises risk, e.g. responsible use of online discussions, etc? • Can they create strong passwords and manage them so that they remain strong? • Can they independently, and with regard for e-safety, select and use appropriate communication tools to solve problems by collaborating and communicating with others within and beyond school? • Can they competently use the internet as a search tool? • Can they reference information sources? • Can they use appropriate strategies for finding, critically evaluating, validating and verifying information, e.g. using different keywords, skim reading to check relevance of information, cross checking with different websites or other non ICT resources? • Can they use knowledge of the meaning of different domain names and common website extensions (e.g. .co.uk; .com; .ac; .sch; .org; .gov; .net) to support validation of information?