

The Catholic School of Saint Gregory The Great

Believe and Achieve



ONLINE SAFETY/ACCEPTABLE USE POLICY AND PROCEDURES

To be read in conjunction with all other policies.

To be reviewed by September 2025
(including updates from KCSIE 2023)

Mission Statement

Believe and Achieve

“We are a safe and happy school where we all shine as part of God's family.”

Online-safety encompasses Internet technologies and electronic communications including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of Digital technologies within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Live streaming
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality e.g. I Pads

It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The previous Computing Policy has been revised and resubmitted as two policies, an Acceptable Use / Online-safety Policy and Computing Teaching and Learning Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's Online-safety Policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Security.

End to End Online-safety

Online-safety depends on effective practice at a number of levels:

- Responsible use of information and digital technologies by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of Online-safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the South West Grid for Learning (SWGFL) including the effective management of SWGFL filtering.
- National Education Network standards and specifications.

School Online Safety Policy

1. Writing and reviewing the Online Safety Policy

The Online Safety Policy relates to other policies including those for Computing, Bullying and for Child Protection/Safeguarding.

- The school will appoint an Online Safety Leader. Our Online Safety Policy has been written by the school, building on government guidance. It has been agreed by Senior Leaders and approved by Governors.
- The Online Safety Policy and its implementation will be reviewed annually.
- The Online Safety Policy was revised by: C Blanch (DSL).....
- It was approved by the Governors on: September 2023... ..

2. Foundation Concepts

- 2.1 Access to information and digital technologies and computer networks owned by The Catholic School of Saint Gregory the Great and access to the internet and e-mail using these resources is conditional on observance of the following Rules for Responsible Use of Information and Digital Technologies (see Appendix 2 and 3).
- 2.2 The Rules for Responsible Use of Information and Digital Technologies have been written by the School's Computing Subject Leader, building on government guidance. They have been agreed by the school's senior staff and approved by Governors and will be reviewed annually.
- 2.3 It is the policy of the school that access to information and digital technologies, computer networks, the internet and e-mail is provided to staff and pupils as a privilege rather than a right. This privilege may be withdrawn at any time in line with these rules.
- 2.4 The Rules for Responsible Use of Digital Technologies apply at all times to all users, in and out of school hours, whilst using school equipment.
- 2.5 It is a general expectation that The Catholic School of Saint Gregory the Great's Computing resources are to be used in a reasonable, efficient, ethical, moral, and legal manner in accordance with the Mission Statement, values, understandings and beliefs of the school.
- 2.6 All staff and children will have regular and updated online safety training alongside safeguarding training. This will include expectations on staff relating to filtering and monitoring.

3. General Rules

- 3.1 Access to Computing resources will only be provided to staff and pupils who have read and agreed in writing to abide by the Rules for Responsible Use of Information and Digital Technologies. In the case of pupils, parent / guardian permission will also be required.
- 3.2 Users of the school's computer systems are allowed to use the facilities freely for school work.
- 3.3 Individual users of school computing resources are responsible for their own behaviour and actions.
- 3.4 Use of school computing resources including e-mail is not considered to be private and should not be treated as such. School senior staff may monitor computer usage at any time with or without the user's knowledge.
- 3.5 School computing resources are provided for academic use and may not be used for any form of personal business or financial gain.

4. Network Access / Basic Computer Security

- 4.1 Users must access the system using only usernames and class work areas that have been assigned to them. Users are personally responsible for the security of resources and passwords issued to them.
- 4.2 Users must not allow anyone else to access the system using a user name, password or resource issued to them. Users are reminded that if this situation occurs they may be charged with illegal actions carried out by the third party.
- 4.3 Users must not attempt to access the system using someone else's username or password or try to access class areas, resources or facilities which have not been made available to them. "Hacking" is illegal under the Computer Misuse Act.
- 4.4 Any user who becomes aware of a breach of network security, loophole or a breach of the Rules for Responsible Use of Information and Digital Technologies is required to inform the Designated Safeguarding Lead (DSL) immediately.

5. Physical Behaviour & Care of Equipment

- 5.1 Users must not cause any unnecessary noise or disturbance to others, or use facilities in a way that results in degradation or disruption of the service to others. Playing and holding conversations creates noise and stops others using the resources to their full potential.
- 5.2 Users must not eat or drink when using or near Computing resources.
- 5.3 Users must treat with care and respect equipment and resources within the school and at other sites accessed through school facilities. Malicious action or vandalism will result in immediate suspension from school facilities. Never deliberately damage or break anything.

6. Software Usage

- 6.1 Software provided on Computing resources has been carefully selected on the basis of educational value and suitability of content and is subject to strict licensing requirements. For this reason users must not install any software unless previously agreed by the Headteacher or SLT. This includes the downloading of applications and utilities from the internet.
- 6.2 No games of any kind with the exception of approved "edutainment" titles may be used on school computing resources during school hours.
- 6.3 Users accessing software or any services available through school facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.
- 6.4 Computing resources must not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act. Any person wishing to use facilities for such a purpose are required to inform the SLT in advance and comply with any restrictions that the UK Data Protection Registrar may impose concerning the manner in which data may be held or processed.

Teaching and Learning

7. Why Internet use is important

- 7.1 The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- 7.2 Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

8. Internet use will enhance learning

- 8.1 The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- 8.2 Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use as part of their unit Online Safety as well as ongoing learning thread throughout every unit.
- 8.3 Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation, this will be taught using the Elim scheme.
- 8.4 Users are not allowed access to public or unregulated chat rooms or to use instant messaging programs.
- 8.5 The school considers all connections to remote locations on the Internet as Virtual School Trips. Therefore, the rules that apply to conduct on regular school trips also apply to users visiting internet sites. It is important that users realise that they are acting as an ambassador for the school.
- 8.6 With the exception of copyright free pictures and text files, no internet content may be downloaded to or via school computing resources by non-staff users. This includes, but is not limited to, music files, games, screen savers, desktop themes and other software.
- 8.7 As computing resources are shared between users and linked to the school address, for their own protection, pupils are not allowed to use the resources to browse auction sites, make any form of online order or purchase or use internet banking services.

9. Pupils will be taught how to evaluate Internet content

- 9.1 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- 9.2 Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

10. Managing Internet Access

Information System Security

- 10.1 School ICT systems capacity and security will be reviewed annually.
- 10.2 Virus protection will be updated regularly.

11. E-mail

- 11.1 Members of staff will be issued with their own email account.
- 11.2 Users may not use other e-mail accounts on the school system.

12. Published Content and the School Website

- 12.1 The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- 12.2 The Headteacher and Governors will take overall editorial responsibility and ensure that content is accurate and appropriate.

13. Child Protection

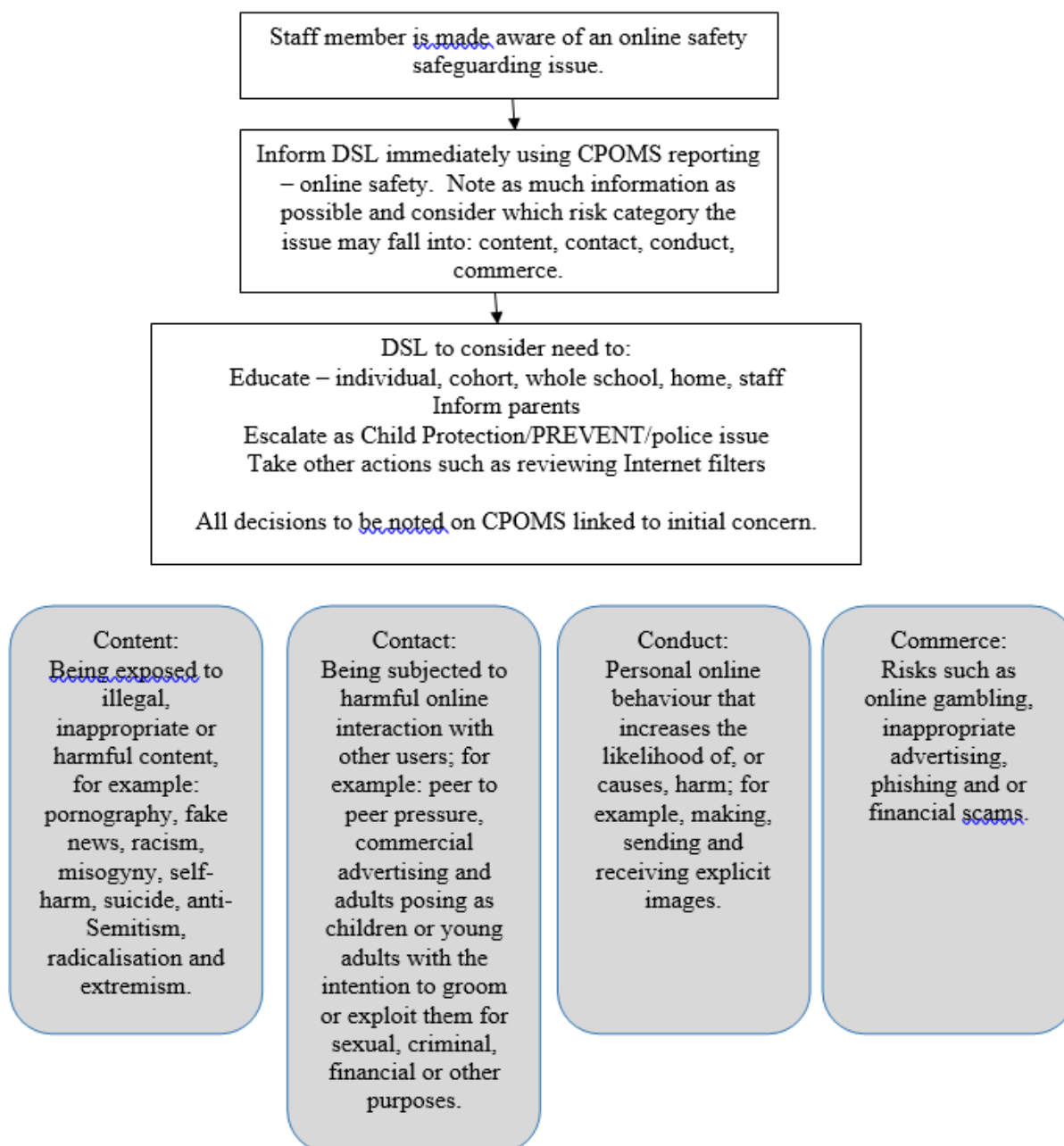
- 13.1 Photographs that include pupils will be selected carefully and pictures will not be used of individual pupils who do not have permission for the web.
- 13.2 Pupils' full names will not be used anywhere on the Website or Blog, particularly in association with photographs, where permission has not been granted.
- 13.3 Written permission from parents or carers will be obtained before photographs of pupils or pupil's work are published on the school Web site and these records will be kept at the office.
- 13.4 It is essential that children are safeguarded from potentially harmful and inappropriate material. When monitoring and educating about online safety, the areas we will focus on are:
 - a) Content: exposure to illegal, inappropriate or harmful content, for example pornography, fake news, racism, misogyny, self-harm, suicide and extremism.
 - b) Contact: being subjected to harmful online interaction with other users, for example peer to peer pressure, commercial advertising and adults posing as children with the intention to groom.
 - c) Conduct: personal online behaviour that increases the likelihood of or causes harm, for example making, sending and receiving explicit images online bullying.
 - d) Commerce: risks such as online gambling, inappropriate advertising, phishing or financial scams.

14. Social Networking and Personal Publishing

- 14.1 The school will block/filter access to social networking sites.
- 14.2 Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- 14.3 Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils and regular reminders will be sent in the newsletter.
- 14.4 Online-safety information evenings will be held on an annual basis in association with the police, when possible.

15. Managing Filtering

- 15.1 The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- 15.2 If staff or pupils discover an unsuitable site, it must be reported immediately to the class teacher and to the Designated Safeguarding Lead.
- 15.3 The DSL will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- 15.4 If inappropriate content/pop-ups/contact takes place online, the following reporting protocol will take place:



16. Managing Emerging Technologies

- 16.1 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- 16.2 Mobile phones will not be allowed in school by pupils unless previously agreed by the Headteacher because children need it for walking home alone. At these times it is off as soon as they enter the school site and then handed to their teacher who will place it into their desk drawer. Whilst teachers will take every possible care to keep the phone safe, the school and/or teachers are not to be held responsible for it. Staff must restrict mobile phone use to outside the classroom and when taking pupils off site.

17. Protecting Personal Data

- 17.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

18. Anti-Virus Precautions

- 18.1 A computer virus is a malicious parasitic program written to alter the way that computers operate without permission or knowledge. They can destroy data, display inappropriate messages or destroy functionality. All school ICT resources are equipped with anti-virus software but home users may not have this, or have an inadequate level of protection.
- 18.2 Viruses spread by copying themselves to other computers via discs as they are loaded on an infected system. For this reason users are not allowed to transfer files to and from school systems and their own equipment by any means other than an encrypted USB which belongs to the school.
- 18.3 Viruses and mal-ware are also spread by attachments on e-mails. Users receiving mail carrying attachments from unknown users or from a known user with an unusual subject line such as "I love you" or "click me" should delete the message without opening it.
- 18.4 The final source of malicious software is internet downloads and pop ups. While most such items will be blocked by the school's filtering system, users should be aware of the existence of these pop ups and avoid clicking on or activating them.
- 18.5 Any deliberate attempt by a user to introduce virus, mal-ware or similar software will be treated in the same way and with the same severity as physical vandalism to school equipment.

19. Policy Decisions

- 19.1 Authorising Internet access
- 19.2 All staff (including volunteers) must read and sign the 'Online safety /Acceptable Use Policy before using any school computing resource.
- 19.3 The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- 19.4 Access to the Internet will be adult led with directly supervised access to specific, approved on-line materials.

20. Assessing Risks

- 20.1 The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences of Internet access.
- 20.2 The school will audit computing provision to establish if the Online-safety Policy is adequate and that its implementation is effective.

21. Handling Online-safety Complaints

- 21.1 Complaints of Internet misuse will be dealt with by a senior member of staff.
- 21.2 Any complaint about staff misuse must be referred to the Headteacher.
- 21.3 Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and immediately reported to the Designated Safeguarding Lead.
- 21.4 Pupils and parents will be informed of the complaints procedure.

22. Communications Policy

Introducing the Online-safety Policy to Pupils

- 22.1 Online-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year and on Internet Safety Day.
- 22.2 Pupils will be taught Online-safety in specific lessons within PSHCE, RSHE and each year group is taught Online-safety focused sessions within their computing curriculum, following the school's scheme of work using educational websites for support such as thinkuknow, childnet and kidscape, etc. Online safety is also threaded through all computing lessons.
- 22.3 Pupils will be informed that network and Internet use will be monitored.

23. Staff and the Online-safety Policy

- 23.1 All staff will be given the School Online-safety Policy and its importance explained.
- 23.2 Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

24. Enlisting Parents' Support

- 24.1 Parents' attention will be drawn to the School Online-safety Policy in newsletters, the School Prospectus and on the school Website.

25. Copyright

- 25.1 Users must not take information from the Internet and pass it off as their own work (plagiarism).
- 25.2 Users must not publish information on the school or other websites that is protected by copyright.
- 25.3 No user may copy programs or data which are copyright or subject to restrictive licence agreements on to removable media or on to computers' hard discs. Users should assume that ALL software is subject to such a restriction.

26. Good Practice

- 26.1 Storage space on the network is limited and all users are requested to ensure that old, unwanted data is removed from their area. Users unsure of what can safely be deleted should ask the Network Manager for advice.
- 26.2 Computing resources are backed up every evening automatically. This means files can be restored if deleted or lost in error. However, if users create and delete files on the same day then a backup will not be available to restore. Copies of particularly important files should be saved on removable media until the evening backup is complete.
- 26.3 Users should save their work regularly (approximately every 15 minutes). The network is very reliable but problems do occur (programs crash, power can fail). If you save your work regularly and the network does fail for any reason, you will have only lost approximately 15 minutes work.

27. Use of Computing Resources Out Of School

- 27.1 Certain users may be allocated computing resources for use outside of school. Equipment so issued is the responsibility of the user to which it is assigned and may be used by that user only. Use by family and friends is not permitted.
- 27.2 When used off school premises, computing resources and their users are still covered by all of the *Rules for Responsible Use of Information and Digital Technologies* including those relating to the installation of software, use of the internet and e-mail.
- 27.3 In exception to 27.2 (above) a user allocated a school laptop may set up a basic dial-up or broadband connection on the machine to allow internet access from home subject to the other *Rules for Responsible Use of Information and Digital Technologies* so long as this does not interfere with the systems operation on the school network. Machines so used will be provided with firewall and anti-malware software to help protect them when used outside of the school's filtered internet environment.
- 27.4 In exception to 27.2 (above) a user allocated a school laptop may install printer driver software necessary to allow use of a home printer so long as this does not interfere with the systems operation on the school network.
- 27.5 Staff who have been trained, may access the school server remotely. The same rules above apply. Remote access should only be via a school device, such as laptop. The connection should be logged off at the end of each remote access session.

28. Disciplinary Action

- 28.1 Any infringement of *Rules for Responsible Use of Information and Digital Technologies* may lead to temporary or permanent suspension of use of Computing resources, internet access or both.
- 28.2 Any alleged infringement will be investigated by the Computing Subject Leader or SLT who can, within their discretion, waive or apply a penalty as the circumstances warrant.
- 28.3 Where the Computing Subject Leader or Designated Safeguarding Lead takes the view that it is a particularly serious case, multiple offences have occurred or the possibility of a criminal offence exists, the matter will be referred to the Headteacher and Governing Body. If it is agreed that it warrants such action, formal disciplinary proceedings will be initiated.

29. Understanding Cyber bullying

- 29.1 Cyber bullying is the use of electronic communication to abuse another person.

- 29.2 It can take place anywhere and involve few or many people.
- 29.3 Anybody can be targeted including pupils and school staff.
- 29.4 It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, unauthorized publication of private information or images etc.

30 Procedures to Prevent Cyber bullying

- 30.1 Staff, pupils, parents and Governors to be made aware of issues surrounding cyber bullying and are fully aware of Keeping Children Safe In Education 2023
- 30.2 Pupils and parents will be urged to report all incidents of cyber bullying to the school
- 30.3 Staff CPD will assist in learning about current technologies
- 30.4 Pupils will learn about cyber bullying through online safety lessons, PSHE, RSHE, assemblies, anti-bullying week activities and other curriculum projects. Visiting speakers will deliver some of this learning
- 30.5 Staff, Governor and Visitors will sign an Acceptable Use Agreement/Code of Conduct **(Appendix 4)**.
- 30.6 Parents will be provided with information and advice on how to combat cyber bullying.
- 30.7 Parents and pupils will be expected to sign an Acceptable Use of Information and Digital Technologies agreement after discussing its meaning with their children **(Appendix 5)**.

31. Online Vulnerability

- 31.1 Procedures to be followed in instances where children have been vulnerable online because of online content, contact, conduct or commerce can be found in Appendix 3 of the Safeguarding Policy.

Appendix 1: Internet Use - Possible Teaching and Learning Activities – currently taught using the Elim scheme as a guide.

Activities	Key Online-safety Issues	Relevant Websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories Folders on Network
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. - SafeSearchKids - Swiggle - CBBC Search -
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. RM Easymail	RM EasyMail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News Info mapper Headline History Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Museum sites, etc. Digital Storytelling BBC – Primary Art Media Gallery SWGFL
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Natural History Museum Imperial War Museum

Appendix 2 Online Safety Policy for KS2 Pupils

We know that using the internet is a really fun and exciting thing to do. To ensure that everyone is safe and happy these are the things I must remember when on the internet:

- If I have any concerns about any online safety issues, I will speak to the Digital Safeguarding Team, my teaching partner, or my teacher.
- I will only use digital technologies in school for school purposes.
- I will not tell other people my passwords.
- I will only open/delete my own files.
- I will not bring software, CDs or ICT equipment into school without permission.
- I will only use the Internet after being given permission from a teacher.
- I will make sure that all digital communication with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will close the screen and tell a teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will not use technology in school time to arrange to meet someone unless this is part of a school project approved by a teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using digital technologies because I know that these rules are to keep me safe.
- I know that the school may check my use of digital technologies and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my online safety.
- I know that if I break the rules I might not be allowed to use a computer/ tablet.

Let's have fun whilst being safe!

Signed (child):

Signed (parent):

Appendix 3 Online Safety Policy for FS/ KS1 Pupils

We know that using the internet is a really fun and exciting thing to do. To ensure that everyone is safe and happy these are the things I must remember when on the internet:

- I will ask a teacher or suitable adult if I want to use the computers.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer/ tablet.

Let's have fun whilst being safe!

Signed (child):.....

Signed (parent):

Appendix 4: Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

Information and digital technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of digital technology. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the School Online safety coordinator.

- I will follow the school's Twitter guidelines when using Twitter for parent/ school communication purposes.
- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not use or install any hardware (including USB sticks) or software without permission from the Online-safety co-ordinators.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in-line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head teacher.
- I will respect copyright and intellectual property rights.
- I will check the privacy settings on my social media profiles at least twice every calendar year to ensure they are of the highest setting.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's Online-safety policy and help pupils to be safe and responsible in their use of digital technologies.
- I will ensure that only children whose parents have given permission for them to use the Internet and computing resources are enabled to do so at school.
- I have read and fully understand my duties with regard Keeping Children Safe In Education 2023 and our school Safeguarding Policy and Procedures.

User Signature

I agree to follow this code of conduct and to support the safe use of information and digital technologies throughout the school

Signature Date

Full Name(printed) Job title:

Appendix 5: Acceptable Use of Information and Digital technologies Agreement

PHOTO PERMISSION / ICT & INTERNET USE FORM

This form will remain valid until your child leaves Saint Gregory's School but you are at liberty at any point to rescind your permission. Please ensure you fill in all sections on this form:

PHOTO PERMISSION (Tick as appropriate)	
I agree that photographs may be taken of my child for use (identified only by their first name) in school publications and the classroom .	Yes / No
I agree that photographs may be taken of my child for use (identified only by their first name) on the school social media sites such as - School Website/ *School Twitter/School Blog/YouTube and on DVD. Please note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.	Yes / No
I consent to my child being photographed by local newspapers and other news media , on the basis that their full name may be published along with the picture. Please note that newspapers will be asked to avoid using the child's full name if their image is put on the newspaper's own website and that this consent will be taken to apply to television images, provided that your child is not named except with your specific agreement.	Yes / No
I give permission for my child's picture/video clips to be placed on a disc and distributed amongst their Year Group . The disk will be distributed with a clear message which states that images on the disc are not to be uploaded and used for any social networking.	Yes / No
I agree to historic pictures of my child remaining on publications/website etc when they have left St Gregory's. No new photos will be used for this purpose after they have left.	Yes / No
ICT & INTERNET USE (Tick as appropriate)	
I have read and explained to my child about the school's "Rules For Responsible ICT Use" (Appendix 2 to E-safety /Acceptable Use Policy, found on the school website) and as the parent or legal guardian of the pupil, I grant permission for him / her to use the internet, e-mail and other ICT facilities at school. I understand that the school will take reasonable precautions to ensure that pupils cannot access inappropriate materials, including the teaching of internet safety skills to pupils, but accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet. I accept responsibility for setting and conveying standards for the above named child to follow when selecting, sharing and exploring information and media, and acknowledge that they will be deemed to be accountable for their own actions.	
Parent/Carer Signature	Date

***Please note our School Twitter account is a closed group meaning only parents of the school have access to. Teachers tweet daily with pictures, info and reminders for each year group.**

Appendix 6:

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The Catholic School of Saint Gregory The Great will try to ensure that students / pupils will have good access to digital technologies to enhance their learning and will, in return, expect the students / pupils to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Parent / Carers Name:

Student / Pupil Name:

As the parent / carer of the above students / pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed:

Date: