Online Safety Policy

God made us all unique
To learn, live and grow
To show care, concern and friendship
To be the best we can
Showing Christ's love in all we do.

Approved by:		**Date:**
Last reviewed on:	December 2021	
Next review due by:	September 2022	

Table of Contents

1.0 Aims

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at St Cuthbert's Catholic Primary School with respect to the use of use of technology, including mobile and smart technology (which include mobile phones and tablets)
- Safeguard and protect the children, staff, volunteers and governors of St Cuthbert's Catholic Primary School.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community, including:

  > Assisting school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.

  > Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.

- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content - being exposed to illegal, inappropriate or harmful content including:

- Pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- exposure to wider age inappropriate content, including social media and gaming.
- Managing online information, knowing how to check authenticity and accuracy of online content, understanding what may cause concern or a threat.

Contact- being subjected to harmful online interaction with other users including:

- Cyber-bullying in all forms including, peer-to-peer pressure or abuse (see Peer on Peer abuse policy)
- Exposure to commercial advertising or misleading content and it's impact on self image
- Identity theft (including 'hacking' or accessing an online account, page or content and sharing passwords) and the use of the distribution of content they own.

Conduct- – personal online behavior that increases the likelihood of, or causes, harm

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being, including the amount of time spent online and the awareness of the impact of online technologies on our self-image and identity.

- Consensual and non-consensual sharing of intimate or explicit images, or communications, also referred to as SGII (self-generated indecent images) or Sexting.
- Use of a range online material, including the use of copyright and other ownership.

1.1 Who will write and review the policy?

Senior Manager with responsibility for whole school ICT:	Headteacher
Safeguarding Responsibility:	Headteacher
Technician:	Newcastle LA- Internet IT Assist- Technology
Computing Governor:	David Hastie

Monitoring of the Computing (Previously ICT) policy is the responsibility of the Computing Leader and Senior Management of the school.

The policy is reviewed each year by the Computing Team and Senior Management Team and fully revised and presented to Governors for final approval every three years before being issued to staff.

As Online Safety is an important aspect of strategic leadership within the school, the Head Teacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety Coordinator in this school is Carolyn Ferguson (Sarah Dorning is acting as the Computing Leader) who has been designated this role as a member of the Senior Management Team. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety Coordinator to keep abreast of current issues and guidance through organisations such as Newcastle Local Authority, Department for Education, Child Exploitation and Online Protection Centre (CEOP), and Childnet.

Senior Management and Governors are updated by the Head Teacher and e-Safety Coordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies:

- Safeguarding and Child Protection
- Health and Safety
- Home - School Agreements
- Behaviour / Pupil Discipline (including the Anti-Bullying Policy)
- PSHE and Citizenship
- Special Educational Needs and Disability Policy
- Computing Policy
- Anti-Radicalisation Policy
- Catholic Values – British Values
- Equal Opportunities
- Sex and Relationships
- Peer-on-Peer Policy

2.0 Roles and Responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the Online-Safety Co-ordinator • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager)

E-Safety Co-ordinator / Designated Child Protection Lead	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• Promotes an awareness and commitment to e-safeguarding throughout the school community
	• Ensures that e-safety education is embedded across the curriculum
	• Liaises with school ICT technical staff
	• To communicate regularly with SLT and the designated safeguarding Governor to discuss current issues, review any incident logs and filtering
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To ensure that an Online safety incident log is kept up to date
	• Facilitates training and advice for all staff
	• Laises with the Local Authority and relevant agencies
	• Is regularly updated in e-safety issues and legislation, 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 and use of social media

Governors / safeguarding governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of safeguarding Governor which includes e-safety • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the safeguarding Governor will include:

Role	Key Responsibilities
	• regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)
Computing Curriculum Leader	• To oversee the delivery of the Online-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly
Network Manager/ Technician	• To report any e-safety related issues that arise, to the e-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • That he keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • The school's policy on web filtering is applied and updated on a regular basis • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Role	Key Responsibilities
Pupils	• Read, understand and adhere to the Code of Conduct for Pupils (Appendix II) (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, and other smart technologies. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
Parents/carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video. • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To access the school website in accordance with the relevant school Acceptable Use Agreement. To consult with the school if they have any concerns about their children's use of technology Parents can seek further guidance on keeping children safe online from the following organisations and websites: • What are the issues? – UK Safer Internet Centre • Hot topics – Childnet International • Parent resource sheet – Childnet International • Healthy relationships – Disrespect Nobody
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Teaching and learning

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Positive aspects of using the Internet in education include:

- Access to world-wide educational resources, including museums and art galleries
- Educational and cultural exchanges between pupils world-wide
- Vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across networks of schools, support services and professional associations
- Improved access to technical support including remote management of networks and access to learning wherever and whenever convenient
- Great for children to develop future job skills as fun hobbies
- Introduces children to the world of commerce and business
- Encourages creativity and individualism
- Children feel they have 'ownership' of the Internet

Negative aspects of using the Internet include:

- Cyber-bullying
- Online privacy and personal information
- Reputation management and 'digital footprint'
- Sexting, grooming, pornography and other inappropriate material including sites which may encourage terror attacks and extreme violence
- Illegal downloads and copyright infringement
- Spam, phishing, viruses and malware
- Children lying about their age to get onto social networking platforms with a 13+ age limit

Our aim is to produce learners who are confident and effective users of technology . We strive to achieve this by:

- Helping all children to use technology with purpose and enjoyment
- Helping all children to develop the necessary skills to exploit technology
- Helping all children to become autonomous users of technology
- Helping all children to evaluate the benefits of technology and its impact on society
- Meeting the requirements of the National Curriculum and helping all children to reach the highest possible standards of achievement
- Using technology to develop partnerships beyond the school
- Celebrating success in the use of ICT

3.1 Pupil e-safety curriculum

St Cuthbert's Catholic Primary School:

- Has a clear, progressive e-safety education programme as part of the Computing Curriculum / RSE Curriculum. This covers a range of skills and behaviours, as outlined in Educating a Connected World, that is appropriate to their age and experience, including:
    - Self-Image and Identity:
        - to understand 'What is the internet?' and the different ways we can connect online.
        - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
        - understanding what is a digital footprint and how we can manage this
    - Online Relationships:
        - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour
        - to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
        -
    - Online reputation:
        - to develop strategies to personalise digital content safely, for example how to create safe and appropriate profiles and effective passwords.
    - Online Bullying:
        - to understand the impact of cyber-bullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
        - to know how to report any abuse including cyber-bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
    - Managing online information:
        - to develop a range of strategies to evaluate and verify information before accepting its accuracy
        - To understand how information can be found, viewed and interpreted.
        - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
        - to know how to narrow down or refine a search;
        - to have strategies for dealing with receipt of inappropriate materials e.g. pornographic images, radicalisation / extremism websites;
        - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - Impact on our Health Wellbeing and lifestyle:
        - to understand the impact technology has on our health, well-being and lifestyle, i.e. limiting screen time, impact on our mood, sleep and relationships with others.
        - to recognise negative behaviours and issues that may be amplified through online research or information i.e. self-harm/suicide/eating disorders, and develop strategies for reporting and dealing with this.

- Privacy and Security:
  - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos
  - to know how to ensure they have turned-on privacy settings;
  - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons
  -
- Copyright and Ownership:
  - to understand why they must not post pictures or videos of others without their permission;
  - to know not to download any files – such as music files - without permission;
  - to understand why they must not post pictures or videos of others without their permission;

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through the Code of Conduct for Pupils which every student will agree to and display copies throughout the school
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online; online gaming / gambling;

3.1 Why is Internet use important?

The Internet is an essential element in 21st century life for education, business and social interaction. Digital literacy skills and knowledge are vital to access life-long learning and employment; indeed these skills are now seen as a functional, essential life-skill along with English and Mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet can benefit the professional work of staff and enhance the school's business administration system.

3.2 How does Internet use benefit education?

Increased computer numbers and improved Internet access may be provided but its impact on pupils' learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and refine their publishing and communications with others via the Internet. It is also used to help children access learning remotely when needed (see Digital Remote Learning Policy). Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- The school's Internet access will be designed to enhance and extend education
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work

3.4 How will pupils learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc provide an opportunity for pupils to develop skills in evaluating Internet content; for example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- The evaluation of online materials is part of teaching/learning in every subject

Managing Content and Communication

4.1 How will email be managed?

- Pupils may only use approved email accounts
- Pupils must immediately tell a teacher if they receive offensive email
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone
- Whole-class or group email addresses will be used for communication outside of the school
- Pupils are not permitted to access personal, external email accounts in school
- The forwarding of chain messages is not permitted
- Staff should not use personal email accounts for professional purposes
- Staff should be aware of their conduct whilst emailing or communicating with children and parents using their designated class email, and understand that this is a written and admissible document.
- Staff must ensure sensitive information is shared safely and appropriately and must report any breaches of data protection immediately.

4.2 School website

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright
- Staff are responsible for links or content shared and uploaded to the website, this includes external links and home learning opportunities.

4.3 Home Learning

- Learning at home now includes the use of a range of online applications. These will be shared with children and the protection of passwords/profiles will be taught. All applications are monitored regularly by class teachers.
- Where remote learning is needed, teachers should refer to the 'Digital Learning Policy' as a guide. Here clear expectation of digital learning can be found.
- Where online communication takes place, e.g. through e-schools discussion, teachers must monitor this daily and children should be made aware of how to report any comments or issues that may arise here.

Pre-recorded and live sessions

These can be recorded in school or at home using any of the office spaces or a neutral space at home. Each teacher who will be providing recorded sessions can use a school laptop, a school iPad or a school webcam. These must be signed for before they are taken home and returned in a good, working condition. (see Employee Equipment Loan Agreement).

- Staff are asked to set up a YouTube account (using school email). This is where videos can be saved and then shared safely.
- When recording teaching sessions to support remote learning, dress and appearance of staff should adhere to the school's code of conduct and policy.
- Videos should not be recorded in bedrooms and should have a neutral background if possible. Once recorded, videos must be played back to check for content before sharing for teaching purposes.
- Staff must not use any electronic device to access any school data at all unless they are using their own or school's networks. This includes emails and CPOMS (GDPR)
- When taking part in live sessions e.g. TEAMS or Zoom, teachers and pupils are made aware of a clear code of conduct they must adhere to. Teacher's should revise this with pupils at the beginning of a session

4.4 Can pupils' images or work be published?

- Parents and carers who take photographs during school productions etc. must not use, share, or publish images or video of pupils without prior consent from the parents and carers of those pupils
- Staff are permitted to take digital/video images of pupils to support educational aims, but must follow school policies concerning the distribution of those images, which should only be taken on school equipment
- When taking digital/video images, ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute

- Images to be published on the school's website, or elsewhere, which include pupils will be selected carefully and will comply with good practice guidance on image use and be used to support the educational aims of the school
- Pupils' names will not be used anywhere on a website, particularly in association with photographs, videos or work unless we have parental/carer permission
- Written permission from parents or carers will be obtained before photographs/videos/work of pupils are published on the school website, or elsewhere (see Appendices V and VI – Photographs of Children Parental Consent Form)

4.6 How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice if classroom use is to be developed.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed

4.7 Mobile Phones and Smart Devices.

Mobile phones, smart watches and tablets are now a feature of modern society and most of our pupils own one. This technology has developed in such a way that they now have the facility to record sound, take photographs and video images. Therefore the school also recognises the advantages that smart devices have as a ubiquitous learning tool. However, this new technology is open to abuse, leading to the invasion of privacy.

Increasing sophistication of smart technology presents a number of issues for schools:

- They are valuable items that may be stolen
- The integration of cameras into phones leading to potential child protection and data protection issues
- The potential to use the device e.g. sending or receiving texts during the school day.

It is our policy to discourage mobile phones and other smart technologies in school however where the parents want the pupil to have a mobile phone with them before and after school, they may do so under the conditions outlined below:

- Phones must always be switched off (not on silent mode) and handed in to the teacher before the start of the school day, to be collected at the end of the day
- If a pupil needs to contact his/her parents/guardians, they will use a school phone in the main office
- If parents need to contact children urgently, they should always phone the school office

- Phones must not be used for any purpose (e.g. phoning, texting, surfing the internet, taking photos, checking the time, taking videos) between the hours of 8.45am and 3.00pm.
- School accepts no responsibility whatsoever for theft, loss, damage or health effects, (potential or actual), relating to mobile phones
- It is the responsibility of parents and pupils to ensure mobile phones are adequately insured
- If a pupil breaches these rules, the phone will be confiscated and given in to the main office. It will be returned to the pupil on receipt of a phone call or email from parents.
- Further action will be taken if mobile phones are used and there are Child Protection implications. The severity of the action from school will depend on the particular circumstances. Appropriate external authorities will be alerted if necessary including Social Services and Police.

4.8 Laptops and other technology

- Staff provided with a laptop purchased by the school can only use it for private purposes at the discretion of the Head Teacher. Such laptops remain the property of the school and are open to scrutiny by senior management, contracted technicians and the Computing subject leader.
- Laptops belonging to the school must have updated antivirus software installed and be password protected. This will be updated on an annual basis by the school.
- Staff intending to bring personal laptops on to the school premises should consider whether this is appropriate. There are security risks associated with any private content on the laptop
- Staff should not attach personal laptops to the school network
- The security of school laptops is of prime importance due to their portable nature and them being susceptible to theft
- Any technology accessed or taken home by staff must be signed in and out in the log found in the school office. This includes the device and all associated attachments.

Policy Decisions

5.1 Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's computers and ICT equipment
- All staff must read and sign the 'Acceptable Use for Staff Agreement' before using any school ICT resource
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific approved online materials
- Parents will be asked to sign and return a consent form for pupil access
- Parents will be informed that pupils will be provided with supervised Internet access (see Appendix II)

5.2 Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material through the use of corporate filtering systems.

- The final decision when assessing risks will rest with the Head Teacher

5.3 Handling e-Safety complaints

- Any e-safety complaints will be dealt with in line with the school complaints policy.
- Any complaint about staff misuse must be referred to the Head Teacher who will decide if sanctions are to be imposed
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- The Head Teacher will arrange contact/ discussions with Newcastle Local Authority and the police to establish clear procedures for handling potentially illegal issues

5.4 Safeguarding and Child Protection

Children and young people can be exploited and suffer bullying through their use of modern technology such as the Internet, mobile phones and social networking sites. In order to minimize the risks to our children and young people St Cuthbert's Catholic Primary School will ensure that we have in place appropriate measures such as security filtering, and an acceptable use policy. E-safety is discussed as an ongoing theme but we also have a specific e-safety focus every year in the Spring Term that coincides with Safer Internet Day. We will also ensure that our children understand the risks associated with going online and being exposed to inappropriate content like pornography, ignoring age ratings on games, substance abuse and sites which encourage terror attacks and extreme violence. We will help them become more resilient to these dangers and know where to go for help and support. This applies to both structured and unstructured times.

We will ensure that staff are educated on the safe use of modern technologies during teaching activities. We will also educate staff about the dangers children can be exposed to online (cited above) both inside and outside of school so that they can be vigilant and proactive in keeping children safe. We will also make staff aware of how not to compromise their position of trust in or outside of the school and make sure they are aware of the dangers associated with social networking sites.

Cyberbullying

Cyberbullying (also known as 'trolling' or internet bullying') is the anti-social act of causing personal conflict and controversy online. It can also include cyberstalking (the repeated unwanted contact or form of communication), online impersonating, doxxing (publishing someone's personal information online as a call for others to harass them) and trolling. It is important that children recognise that criminal legislation can apply to associated behaviours such as criminal harassment, stalking, malicious communications, and disclosing private sexual images.

The Malicious Communications Act states:

Any person who sends a letter, electronic communication or article of any description to a person that conveys a message that is indecent or highly offensive, a threat or false information. If the reason for that communication was to cause distress or anxiety to the recipient or to any other person, then the sender is guilty of an offence.

This includes mobile phones and the Internet (any form of electronic communication).
The offence occurs whether those targeted actually receive the message or not.

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's Anti-Bullying Policy and Peer on Peer Abuse Policy.
- There will be clear procedures in place to support anyone affected by Cyberbullying
- All incidents of Cyberbullying reported to the school will be recorded

There will be clear procedures in place to investigate incidents or allegations of Cyberbullying:

- Pupils, staff and parents/carers will be advised to keep a record of the bullying or peer on peer abuse as evidence
- The school will take steps to identify the perpetrator, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary

Sanctions for those involved in Cyberbullying may include:

- The perpetrator will be asked to remove any material deemed to be inappropriate or offensive
- A service provider may be contacted to remove content
- Internet access may be suspended at school for the user for a period of time
- Parent/Carers may be informed
- The police will be contacted if a criminal offence is suspected

Disseminating the Policy

6.1 Sharing with pupils

- e-Safety rules and posters will be displayed in all rooms where computers are used and highlighted/ discussed during computing lessons
- Pupils will be made aware that the network and Internet use will be monitored and the impact of digital footprints.
- An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use
- e-Safety is embedded in the computing scheme of work for every year group and revisited across units.
- Links are made with online safety through our robust RSE programme
- Internet safety Day will help promote the importance of safe internet use.
- Termly online safety content will be produced and shared with pupils and parents
- The Safeguarding officers will meet termly to discuss issues and share child led videos promote online safety to parents and children.
- Pupils will be made aware of procedures to follow if they come across any inappropriate material on the Internet (including online pornography, online gambling, hate sites, lifestyle websites e.g. pro-anorexia/self-harm/substance abuse /suicide sites, radicalisation / extremism websites.)

6.2 Sharing with staff

- Staff will be consulted when creating and reviewing the e-Safety policy
- Staff training in safe and responsible Internet use, both professionally and personally, will be provided, including use of social networking sites such as Facebook, Twitter and Instagram. The E-Safety Coordinator and Computing Leader do have access to the school social media platforms in school for monitoring purposes.
- Training will also cover the risks posed by the online activity of extremist and terrorist groups
- Every member of staff, whether permanent, temporary or supply, will be informed that Network and Internet traffic will be monitored and can be traced, ensuring individual accountability

6.3 Engaging parents

- Parents'/ carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website
- A parents' workshop will be held annually to inform parents/ carers about e-Safety issues and responsible use
- A termly internet safety newsletter will be shared with parents to highlight prevalent issues.
- The Safeguarding officers will share child led videos promote online safety to parents and children.
- Parents will be requested to sign an e-Safety/Internet agreement as part of the Home School Agreement (Appendix III)
- Information and guidance on e-Safety will be made available to parents/carers in a variety of formats (i.e. weblinks, printed documents, leaflets, presentations)

Incident Management

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues

- monitoring and reporting of e safety incidents takes place and contributes to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- we will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

Acceptable Use Agreement for Staff

ICT and the related technologies such as e-mail, the Internet and mobile devices form part of our daily life within school. To ensure that all adults within the school setting are aware of their responsibilities when using any form of ICT all staff must sign this Acceptable Use Agreement and adhere to its content at all times. This is to ensure staff provide positive role models to pupils for the safe and responsible use of online technologies and also safeguard themselves from any potential allegations or inadvertent misuse.

- I know that I should only use the school equipment in an appropriate manner and for professional use in accordance with the e-Safety Policy
- I will not give out personal information (mobile phone number, personal e-mail address or social networking sites e.g. Facebook, Twitter or Instagram) to pupils or parents or allow any personal information to be easily accessible
- I will only use the approved, secure e-mail system (name@schoolname.newcastle.sch.uk, classstcuthbertsk@outlook.com) for any school business
- I will ensure the school office has the password for the class email in case of staff illness / absence
- I know that I should complete virus checks on my laptop, memory stick and other portable devices so that I do not inadvertently transfer viruses onto the school network or other ICT equipment
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will ensure school data is stored securely and used appropriately in accordance with school and other relevant policies
- I will not save any school information or data concerning children on my memory stick
- I will not save photographs or videos of children on my memory stick
- I will report any accidental misuse of school ICT, or accidental access to inappropriate material, to the ICT Subject Leader or Head Teacher
- I will not connect any personal device (laptop, digital camera etc), to the school network without authorisation from the Head Teacher
- I will respect copyright and intellectual property laws
- I understand that all my use of the Internet and other related technologies can be monitored and logged and made available to the Head Teacher
- I will ensure that my online activity, both in and outside school, will not bring myself or the school into disrepute (this includes postings on social networking sites e.g. Facebook, Twitter and Instagram)
- I will not discuss any school business on any social media websites

Mobile Phones in School

- I will keep my phone turned off during teaching sessions and ensure that it is secured in a bag or desk drawer
- If I need to use my phone in school I will do so in a private room where there is no other adult or child present

Mobile Phones on Day Trips and Residential Visits

- I will only use my phone for contact with school and other staff on the residential / day trips.
- If I need to use my mobile phone for personal reasons, I will only do so after prior discussion with the trip leader and senior management and I will use it discretely.

I have read, understood and agree to this code of conduct. I will support the safe and secure use of ICT throughout the school. I am aware I may face disciplinary action if I fail to adhere to it.

I understand that this information will be held in compliance with our retention policy.

Signature: _____ Date: _____

Print Name: _____

Code of Conduct for Pupils

E-Safety Code of Conduct for Pupils

I agree to follow these rules when using the Internet:

- I will not share my username, password or personal information with anyone else
- I will make sure that ICT communication with other users is responsible, polite and sensible
- I will not look for, save or send anything that could be upsetting or cause offence. If I accidentally find anything like this I will tell a teacher immediately
- I will not deliberately misuse or deface other users' work on the school network
- I know that my use of the Internet is monitored and further action may be taken if a member of school staff is concerned about my safety
- I will not play on games which are not age appropriate
- I will be responsible for my behaviour when using the Internet because I know that these rules are designed to keep me safe
- I will recognise dangers and keep myself safe at all times
- If I do not feel safe at any time, I will tell my parents/carers or teachers
- As a child under the age of 13, I understand that I am under the legal age to create an account on Facebook, Twitter, Instagram and TikTok
- I understand that comments made online (e.g. via email, Instant Messenger, Xbox Live, Twitter, Instagram, Snapchat, WhatsApp, TikTok or Facebook) can be hurtful and cause distress and this would not be in keeping with the ethos of our school
- I understand that parents will be informed immediately if any violations of this code of conduct (e.g. name calling) are brought to the attention of the school
- I will keep my phone switched off (not on silent mode) and hand it in to the teacher before the start of the school day and collect it at the end of the day
- I understand and agree to the rules above and am aware there may be sanctions if I do not follow them

Employee Equipment Loan Agreement

To borrow information technology equipment -including but not limited to laptop computers, Ipads, USB cameras -from the school, the employee must read and sign this document, agreeing to the terms as stated:

I understand that this equipment is provided to me for instructional and/or administrative purposes and solely for the completion of my job requirements at St Cuthbert's Catholic Primary School.

I agree to use the equipment in a legal and ethical manner, abiding by all aspects of all local authority and national laws.

I understand that downloading and sharing unlicensed audio and video content violates copyright laws and is prohibited.

I understand that I may not install personal software, change system settings, or tamper with the hardware or existing software.

I agree that I will not leave the laptop unattended at any time, and I will protect it from damage.

I agree to return the equipment to the ICT suite when software installation and/or repairs are necessary.

I agree to return all equipment in working condition upon termination of employment.

I understand that this agreement, which will be kept on file at the school, is binding and enforceable during the entire period in which I have equipment privileges at St Cuthbert's Catholic Primary School

Signature:_____

Print Name: _____

Date: _____

Mobile Phone Policy

- St Cuthbert's Catholic Primary School discourages pupils from bringing mobile phones to school.

- Phones must always be switched off (not on silent mode) and handed in to the teacher before the start of the school day, to be collected at the end of the day.

- The phone must be concealed whilst leaving the school premises.

- Where a pupil is found with a mobile in school, including the playground, the phone will be taken from the pupil and placed in the office. Parents will be contacted to collect the phone.

- If a pupil is found taking photographs or video footage with a mobile phone of either pupils or teachers, this will be regarded as a serious offence and the Head Teacher will decide on appropriate disciplinary action. In certain circumstances, the pupil may be referred to the Police. If images of other pupils or teachers have been taken, the phone will not be returned to the pupil until the images have been removed by an appropriate person.

- Parents are advised that St Cuthbert's accepts no liability for the loss or damage to mobile phones which are brought into the school. It is the responsibility of parents and pupils to ensure mobile phones are adequately insured.

- If a pupil needs to contact his/her parents/guardians, school will do this for them.If parents need to contact children urgently they should phone the school office and a message will be relayed promptly.

Photographs of Children (EYFS)
Consent Form

Name of Pupil …….. Year ……

Dear parents / carers,

At St Cuthbert's we regularly take photographs of pupils. We use these photos in the school brochure, on the school's website, Twitter and Facebook and on display boards around school. The majority of school photographs are kept as a historical record of the life of the school.

We would like your consent to take photos of your child, and use them in the ways described above.

Please tick the relevant box(es) below and return this form to school.

I am happy for the school to take photographs and videos of my child for the sole use of the school. ☐

I am happy for photos of my child to be used in internal displays. ☐

I am happy for photos of my child to be used in the school brochure. ☐

I am happy for photos of my child to be used on the school website. ☐

I am happy for photos of my child to be used on the school's social media sites (Twitter and Facebook). ☐

I am happy for photographs/footage and details of my child being used for press releases for local and/or national newspapers and television broadcasts. ☐

I agree that the electronic learning journey is for my own personal use and not to be shared on social media. This is because my child's learning journey may contain photographs of children whose parents do not wish to have their child's pictures shared on social media. ☐

I understand and agree to group photographic observations. These observations will be shared with the families of children who are in the photograph. ☐

I am **NOT** happy for the school to take or use photos of my child. ☐

I understand that this consent form will be retained by the school on my child's file until they leave this school. ☐

Why are we asking for your consent again?

You may be aware that there are new data protection rules coming in from May. To ensure we are meeting the new requirements, we need to re-seek your consent to take and use photos of your child. We really value using photos of pupils, to be able to showcase what pupils do in school and show what life at our school is like to others, so we would appreciate you taking the time to give consent again.

Furthermore, you may withdraw consent at any time using the Consent Withdrawal Form on the GDPR section of our school website. Paper copies are available from the school office. If you do decide to withdraw consent, the withdrawal will be applied from the date on which the school receives the completed Consent Withdrawal Form.

Date: _____

Parent or Carer's signature: _____

Photographs of Children (Year 1 – Year 6)
Consent Form

Name of Pupil …….. Year ……

Dear Parents /Carers,

At St Cuthbert's we regularly take photographs of pupils. We use these photos in the school brochure, on the school's website, Twitter and Facebook, on display boards around school and in children's books. The majority of school photographs are kept as a historical record of the life of the school.

We would like your consent to take photos of your child, and use them in the ways described above.

Please tick the relevant box(es) below and return this form to school.

I am happy for the school to take photographs and videos of my child for the sole use of the school. ☐

I am happy for photos of my child to be used in internal displays. ☐

I am happy for photos of my child to be used in children's school books. ☐

I am happy for photos of my child to be used in the school brochure. ☐

I am happy for photos of my child to be used on the school website. ☐

I am happy for photos of my child to be used on the school's social media sites (Twitter and Facebook). ☐

I am happy for photographs/footage and details of my child being used for press releases for local and/or national newspapers and television broadcasts. ☐

I am **NOT** happy for the school to take or use photos of my child. ☐

I understand that this consent form will be retained by the school on my child's file until they leave this school. ☐

Date: _____

Parent or Carer's signature: _____

Why are we asking for your consent again?

You may be aware that there are new data protection rules statutory from May 2018. To ensure we are meeting the new requirements, we need to re-seek your consent to take and use photos of your child. We really value using photos of pupils, to be able to showcase what pupils do in school and show what life at our school is like to others, so we would appreciate you taking the time to give consent again.

Furthermore, you may withdraw consent at any time using the Consent Withdrawal Form on the GDPR section of our school website. Paper copies are available from the school office. If you do decide to withdraw consent, the withdrawal will be applied from the date on which the school receives the completed Consent Withdrawal Form.

Appendix VII

Legal Requirements

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation, in England and Wales.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as “Sexting”). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should already have a copy of “Children & Families: Safer from Sexual Crime” document as part of their child protection packs.

More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 - 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files)
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks)

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include racist, xenophobic and homophobic comments, messages etc.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission.
The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.
It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.
It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 - 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material, with a view of releasing it, a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.
This also includes incidents of racism, xenophobia and homophobia.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.
Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008
Section 63 offence to possess “extreme pornographic image”
63 (6) must be “grossly offensive, disgusting or otherwise obscene”
63 (7) this includes images of “threats to a person’s life or injury”
Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006
Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

- Head Teachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site
- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy

This policy became operational from December 2021
The policy may be amended from time to time in accordance with school development and any changes to legislation.