ST CUTHBERT MAYNE SCHOOL

Joint Catholic and Church of England 11-18 Comprehensive School

Dioceses of Plymouth and Exeter

St Cuthbert Mayne School

Online Safety Policy

Adopted by Ethos Committee:	**May 2023**
Reviewed by Full Governing Body:	**July 2023**
Next Review Date:	**May 2024**

Background / Rationale

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

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

The requirement to ensure that young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the School are bound. An Online Safety Policy should help to ensure safe and appropriate use of electronic devices and ICT systems. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leadership team and classroom teachers, support staff, volunteers, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the School. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world.

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

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

Policy Statement

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed) and the use of school chromebooks.

This Online Safety Policy outlines the commitment of St Cuthbert Mayne School to safeguard members of our school community online in accordance with statutory guidance and best practice.

The governors are working with staff, students and parents to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential online safety risks.

The Education and Inspections Act 2006 and the Government's White Paper 'The Importance of Teaching' empowers headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the School.

The School will deal with such incidents within this Policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Schedule for monitoring, development and review of the Online Safety Policy

This Online Safety Policy was approved by St Cuthbert Mayne's Governing Body (Ethos)	*25.05.23*
The implementation of this Online Safety Policy will be monitored by	*Mrs S Walker, Designated Safeguarding Lead*
Monitoring will take place at regular intervals	*Once per year*
The *governing body* will receive a report on the implementation of the Online Safety Policy and include details of online safety incidents at regular intervals	*Ethos Governors meetings held 3 times per year*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be	*May 2024*

Should serious online safety incidents take place, the following external persons/agencies should be informed, dependant upon case by case basis and nature of incident	*Police, including cyber crime unit if necessary; social care; MASH, Action Fraud*

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using;

- Log of reported incidents via CPOMS
- Monitoring of logs of internet activity - Smoothwall monitoring system
- Internal monitoring of data for internal activity
- Surveys/questionnaires from learners/staff/parents

Policy & Leadership

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and senior leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Designated Safeguarding Lead (DSL)/DDSLs.

- The Headteacher and the Designated Safeguarding Lead (DSL) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Headteacher and the Designated Safeguarding Lead (DSL) are responsible for ensuring that relevant staff receive suitable JPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Headteacher/senior leaders are responsible for ensuring that the DSL (Online Safety Lead), technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

- The DSL/DDSLs should actively promote awareness of online safety and good practice within the school community as a whole.

- The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

Governors

The DfE guidance ‘Keeping Children Safe in Education’ states:

‘Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children’s welfare … This includes … online safety’.

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of this policy.

The governors will:

- Discuss, monitor and review the Online safety and related policies on an annual basis.
- Support staff in the use of ICT as an essential tool for enhancing learning and in the embedding of e-safety across the whole curriculum.
- Ensure that students are aware, through online safety education, of the potential online safety risks associated with the use of ICT and mobile technologies, that all online safety concerns will be dealt with sensitively and effectively; that students feel able and safe to report incidents; and that students abide by the School’s Online Safety Policy.
- Provide opportunities for parents/carers to receive online safety education and information, to enable them to support their children in developing good online safety behaviour. The School will report back to parents/carers regarding online safety concerns.
- Seek to learn from online safety good practice elsewhere and utilise the support of the Trust, SWGfL and relevant organisations when appropriate.

Online Safety Lead (DSL/DDSL)

The Online Safety Lead will:

- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns

- have a leading role in establishing and reviewing the school online safety policies/documents

- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond

- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated

- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents

- receive reports of online safety incidents[1] and create a log of incidents to inform future online safety developments

Should be trained in online-safety issues and be aware of the potential for serious child protection issues to arise from:

Sharing of personal data; access to illegal/inappropriate materials; inappropriate on-line contact with adults/strangers; potential or actual incidents of grooming; cyber-bullying

Network Manager:

The Network Manager is responsible for ensuring:

That they are aware of, and follow, the School’s Online Safety Policy and carry out their work effectively in line with the policy.

- that the School’s ICT infrastructure is secure and is not open to misuse or malicious attack;
- that the School meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance;
- that users may only access the School’s networks through a properly enforced password protection policy, in which passwords are regularly changed;
- SWGfL is informed of issues relating to the filtering applied by the Grid;
- the School’s filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- that the online safety technical information is kept up to date in order to effectively carry out their e-safety role and to inform and update others as relevant;
- that the use of the Network, Virtual Learning Environment (VLE), remote access, email is regularly monitored in order that any misuse or attempted misuse can be reported to the Designated Safeguarding Lead for investigation;
- that monitoring software/systems are implemented and updated as agreed in School policies.

Teaching and Support Staff:

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem in the appropriate manner (as per safeguarding flowchart) for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand online safety and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource

- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc

- to model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

- are 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, including Staff Code of Conduct.

Students:

- are responsible for using the School ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to School systems;
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand School policies on the use of mobile phones,digital cameras and hand held devices, they should also know and understand School policies on the taking/use of images and on cyber-bullying;
- should 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.

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed)

- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- should know what to do if they or someone they know feels vulnerable when using online technology

should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. ***"There is a generational digital divide". (Byron Report).***

The School will therefore take every opportunity to help parents understand these issues through;

- publishing the Online Safety Policy on the school website
- providing a copy of the learner's acceptable use agreement

- publish information about appropriate use of social media relating to posts concerning St Cuthbert Mayne School
- seeking their permissions concerning digital images
- parents/carers evenings, newsletters, website, social media and information about national, local online safety campaigns, such as 'Safer Internet Day'.
- publishing information from The National College on the school website to support parents in developing their knowledge of games and social media platforms.

Parents and carers will be encouraged to support the school in reinforcing the online safety messages provided to the learners in school and the use of their children's personal devices in the school (St Cuthbert Mayne School is a mobile free site and parents will be asked to encourage their children in reinforcing this policy).

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Any illegal activity for example: · Child sexual abuse imagery* · Child sexual abuse/exploitation/grooming · Terrorism · Encouraging or assisting suicide · Offences relating to sexual images i.e., revenge and extreme pornography · Incitement to and threats of violence · Hate crime · Public order offences - harassment and stalking · Drug-related offences · Weapons / firearms offences · Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X

Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	· Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) · Gaining unauthorised access to school networks, data and files, through the use of computers/devices · Creating or propagating computer viruses or other harmful files · Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) · Disable/Impair/Disrupt network functionality through the use of computers/devices · Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information here					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	

	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

POLICY STATEMENTS

Education – students:

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the School's online safety provision. Young people need the help and support of the School to recognise and avoid online safety risks and build their resilience.

Online Safety education will be provided in the following ways:

- A planned online safety programme should be provided as part of ICT: this will cover both the use of ICT and new technologies in School and outside School.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

Education and Training – Staff:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the School Online Safety policy and Acceptable Use Policies.
- The Designated Safeguarding Lead/Network Manager will receive regular updates through attendance at SWGfL/the Trust/other information/training sessions and by reviewing guidance documents released by BECTA (British Educational Communication & Technology Agency)/SWGfL /LA and others.
- The Designated Safeguarding Lead and DDSLs will provide advice/guidance/training to individuals as required.

Training – Governors:

Training/awareness sessions should be available to Governors, with particular importance for those who are members of any committee/group involved in ICT Online safety/health and safety/child protection. This may be offered by participation in School training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring:

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

- School ICT systems will be managed in ways that ensure that the School meets the Online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety guidance.
- There will be regular reviews and audits of the safety and security of School ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to School ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager
- All users will be provided with a username and password by the network manager who will keep an up to date record of users and their usernames. Users will be required to change their password every term.
- The "master / administrator" passwords for the School ICT system, used by the Network Manager must also be available to the Headteacher or Assistant Headteacher i/c ICT and kept in a secure place (e.g. School safe).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The School maintains and supports the managed filtering service provided by SWGfL and monitoring system by Smoothwall
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader). Any filtering issues should be reported immediately to SWGfL.
- School ICT technical staff regularly monitor and record the activity of users on the School ICT systems and users are made aware of this in the Acceptable Use Policy.
- Personal data cannot be sent over the internet or taken off the School site unless safely encrypted or otherwise secured.

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, eg on social networking sites.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Photographs of students will not be published on the school website or any other media tool if consent has been declined.
- Students' work can only be published with the permission of the student and parents or carers.

Please refer to the St Cuthbert Mayne School Use of Images Policy for further information

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

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

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- No personal data is stored on any portable computer system, USB stick or any other removable media.
- Transfer data using encryption and secure password protected devices.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the School currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	STAFF & OTHER ADULTS				**STUDENTS**			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to School	✔				✔			
Use of mobile phones in lessons				✔			✔	
Use of mobile phones in social time	✔							✔
Taking photos on mobile phones or other camera devices							✔	
Use of personal email addresses in School, or on School network				✔				✔
Use of chat rooms / facilities				✔				✔
Use of social networking sites in social time	✔							✔
Use of blogs	✔					✔		

When using communication technologies the School considers the following as good practice:

- The official School email service may be regarded as safe and secure and is monitored.

- Users must immediately report, to their Line Manager/Tutor/Year Coordinator, in accordance with the School policy, the receipt of any email that makes them feel uncomfortable, is offensive, intimidating, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents/carers (via email, etc) must be professional in tone and content. These communications may only take place on official (monitored) School systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Personal information should not be posted on the School website or Facebook/Twitter page and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from School and all other ICT systems. Other activities eg Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a School context, either because of the age of the users or the nature of those activities.

The School believes that the activities referred to in the following section would be inappropriate in a School context and that users, as defined, should not engage in these activities in School or outside School when using School equipment or systems.

Responding to incidents of misuse

It is hoped that all members of the School community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity, for example:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

the SWGfL flow chart – at http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such an event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

Staff must always report any safeguarding concerns via CPOMS (or the pink slip available in departments/google docs/staff room - for non-CPOMS users) immediately to:

Designated Safeguarding Lead

- Safeguarding allegation against an adult

Deputy Designated Safeguarding Leads

- All other safeguarding concerns

Headteacher

- Safeguarding allegation against a member of staff