St Cuthbert's
Catholic High School

Live life in all its fullness

Online Safety Policy

2020/21

Person responsible for Policy:	Senior Leadership Team
Committee responsible for Policy:	Pastoral & Personal Development
Date To Governors:	February 2021
Date Agreed:	February 2021
Review Due:	September 2021 and annually thereafter
Is this Policy to appear on school website:	Yes

Contents:

Statement of intent

St Cuthbert's Catholic High School understands that using online services is an important aspect of raising educational standards, promoting student achievement and enhancing teaching and learning.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of students and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

The measures implemented to protect students and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

Signed by:

	Headteacher	Date:	
	Chair of governors	Date:	

1. Legal framework

1.1. This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2020) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety 'Education for a Connected World'
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'

1.2. This policy operates in conjunction with the following school policies:

- Anti-Bullying, Harassment and Hate Incidents Policy (including Cyberbullying)
- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement
- Data and E-Security Breach Prevention and Management Plan
- Child Protection and Safeguarding Policy
- PSHE Policy
- RSE and Health Education Policy
- Searching, Screening and Confiscation Policy
- Students' Personal Electronic Devices Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Confidentiality Policy
- Photography Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy

2. Roles and responsibilities

2.1. The **governing board** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an **annual** basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.

2.2. The **headteacher** is responsible for:

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping students safe.
- Working with the **DSL and ICT engineers** to conduct **half-termly** light-touch reviews of this policy.
- Working with the **DSL and governing board** to update this policy on an **annual** basis.

2.3. The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT engineers.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.

- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the **governing board** about online safety on a **termly** basis.
- Working with the **headteacher and ICT engineers** to conduct **half-termly** light-touch reviews of this policy.
- Working with the **headteacher and governing board** to update this policy on an **annual** basis.

2.4. **ICT engineers** are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the **headteacher**.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the **DSL and headteacher** to conduct **half-termly** light-touch reviews of this policy.

2.5. All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

2.6. Students are responsible for:

- Adhering to this policy, the **Acceptable Use Agreement** and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. The curriculum

3.1. Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSE
- Healthy Living education
- Active Form time
- Personal development including PSHE and Citizenship
- Computing

3.2. The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.

3.3. Students are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

3.4. Online safety teaching is always appropriate to students' ages and developmental stages.

3.5. The underpinning knowledge and behaviours students learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

3.6. The online risks students may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix 1 of this policy.

3.7. The DSL is involved with the development of the school's online safety curriculum.

3.8. The school recognises that, while any student can be vulnerable online, there are some students who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. students with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these students receive the information and support they need.

3.9. Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?

- What is their background?
- Are they age appropriate for students?
- Are they appropriate for students' developmental stage?

3.10. External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The **headteacher and DSL** decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

3.11. Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that students in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any student who may be especially impacted by a lesson or activity.

3.12. Lessons and activities are planned carefully so they do not draw attention to a student who is being or has been abused or harmed online, to avoid publicising the abuse.

3.13. During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which students feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

3.14. If a staff member is concerned about anything students raise during online safety lessons and activities, they will make a report in line with sections 15 and 16 of this policy.

3.15. If a student makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in sections 15 and 16 of this policy.

4. Staff training

4.1. All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

4.2. Online safety training for staff is updated annually and is delivered in line with advice from local safeguarding partners and National Online Safety.

4.3. In addition to this training, staff also receive regular online safety updates as required and at least annually.

4.4. The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training through National Online Safety. This training is updated at least every two years.

4.5. In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep students safe while they are online at school.
- Recognise the additional risks that students with SEND face online and offer them support to stay safe online.

4.6. All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

4.7. Staff are required to adhere to the **Staff Code of Conduct** at all times, which includes provisions for the acceptable use of technologies and the use of social media.

4.8. All staff are informed about how to report online safety concerns, in line with sections 15 and 16 of this policy.

4.9. The DSL acts as the first point of contact for staff requiring advice about online safety.

5. Educating parents

5.1. The school works in partnership with parents to ensure students stay safe online at school and at home.

5.2. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

- Online Safety for Parents courses from National Online Safety
- School website
- Social media posts

5.3. Parents are sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

6. Classroom use

6.1. A wide range of technology is used during lessons, including the following:

- Smartphones
- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras

6.2. Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that students use these platforms at home, the class teacher always reviews and evaluates the resource.

6.3. **Class teachers** ensure that any internet-derived materials are used in line with copyright law.

6.4. Students are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

7. Internet access

7.1. Students, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

7.2. A record is kept of users who have been granted internet access on the shared drive on the school's ICT network.

7.3. All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

8. Filtering and monitoring online activity

8.1. The governing board ensures the school's ICT network has appropriate filters and monitoring systems in place.

8.2. The headteacher and ICT engineers undertake a risk assessment to determine what filtering and monitoring systems are required.

8.3. The filtering and monitoring systems the school implements are appropriate to students' ages, the number of students using the network, how often students access the network, and the proportionality of costs compared to the risks.

8.4. The governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

8.5. ICT engineers undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

8.6. Requests regarding making changes to the filtering system are directed to the headteacher.

8.7. Prior to making any changes to the filtering system, ICT engineers and the DSL conduct a risk assessment.

8.8. Any changes made to the system are recorded by ICT engineers.

8.9. Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

8.10. Deliberate breaches of the filtering system are reported to the DSL and ICT engineers, who will escalate the matter appropriately.

8.11. If a student has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy.

8.12. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

8.13. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

8.14. The school's network and school-owned devices are appropriately monitored.

8.15. All users of the network and school-owned devices are informed about how and why they are monitored.

8.16. Concerns identified through monitoring are reported to the DSL who manages the situation in line with sections 15 and 16 of this policy.

9. Network security

9.1. Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT engineers.

9.2. Firewalls are switched on at all times.

9.3. ICT engineers review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

9.4. Staff and students are advised not to download unapproved software or open unfamiliar email attachments.

9.5. Staff members and students report all malware and virus attacks to ICT engineers.

9.6. All members of staff have their own unique usernames and private passwords to access the school's systems.

9.7. Students in class year or key stage and above are provided with their own unique username and private passwords.

9.8. Staff members and students are responsible for keeping their passwords private.

9.9. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

9.10. Passwords expire after 90 days, after which users are required to change them.

9.11. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.

9.12. Users are required to lock access to devices and systems when they are not in use.

9.13. Users inform ICT engineers if they forget their login details, who will arrange for the user to access the systems under different login details.

9.14. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.

9.15. Full details of the school's network security measures can be found in the Data and E-Security Breach Prevention and Management Plan.

10. Emails

10.1. Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement and Confidentiality Policy.

10.2. Staff and students are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours.

10.3. Prior to being authorised to use the email system, staff and students must agree to and sign the relevant acceptable use agreement.

10.4. Personal email accounts are not permitted to be used on the school site.

10.5. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

10.6. Staff members and students are required to block spam and junk mail, and report the matter to ICT engineers.

10.7. The school's monitoring system (Securus) can detect inappropriate links, malware and profanity within emails – staff and students are made aware of this.

10.8. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

10.9. Any cyberattacks initiated through emails are managed in line with the Data and E-Security Breach Prevention and Management Plan.

11. Social networking

Personal use

11.1. Access to social networking sites via the school's WiFi is filtered as appropriate for both staff and students.

11.2. Staff and students are not permitted to use social media for personal use during lesson time.

11.3. Staff can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action.

11.4. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

11.5. Staff receive annual training on how to use social media safely and responsibly.

11.6. Staff are not permitted to communicate with students or parents over social networking sites and are reminded to alter their privacy settings to ensure students and parents are not able to contact them on social media.

11.7. Students are taught how to use social media safely and responsibly through the online safety curriculum.

11.8. Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy.

Use on behalf of the school

11.9. The use of social media on behalf of the school is conducted in line with the Social Media Policy.

11.10. The school's official social media channels are only used for official educational or engagement purposes.

11.11. Staff members must be authorised by the headteacher to access to the school's social media accounts.

11.12. All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

11.13. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

12. The school website

12.1. The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

12.2. The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

12.3. Personal information relating to staff and students is not published on the website.

12.4. Images and videos are only posted on the website if the provisions in the Photography Policy are met.

13. Use of school-owned devices

13.1. Staff members are issued with the following devices to assist with their work:

- Laptop
- Tablet
- Phone

13.2. Students are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.

13.3. School-owned devices are used in accordance with the Device User Agreement.

13.4. Staff and students are not permitted to connect school-owned devices to public Wi-Fi networks.

13.5. All school-owned devices are password protected.

13.6. All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen.

13.7. All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

13.8. ICT engineers review all school-owned devices on a monthly basis to carry out software updates and ensure there is no inappropriate material on the devices.

13.9. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT engineers.

13.10. Staff members or students found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behaviour Policy.

14. Use of personal devices

14.1. Personal devices are used in accordance with the Staff ICT Acceptable Use and Bring Your Device (BYOD) Policy and the Students' ICT Acceptable Use and Bring Your Device (BYOD) Policy.

14.2. Any personal electronic device that is brought into school is the responsibility of the user.

14.3. Staff members are not permitted to use their personal devices during lesson time, other than in an emergency.

14.4. Staff members are not permitted to use their personal devices to take photos or videos of students.

14.5. Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy.

14.6. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the **headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.**

14.7. Students are not permitted to use their personal devices during lesson time (unless permission is expressly given by the class teacher) or when moving between lessons.

14.8. If a student needs to contact their parents during the school day, they are allowed to use the phone in the school office.

14.9. The headteacher may authorise the use of mobile devices by a student for safety or precautionary use.

14.10. Students' devices can be searched, screened and confiscated in accordance with the Searching, Screening and Confiscation Policy.

14.11. If a staff member reasonably believes a student's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

14.12. Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices.

14.13. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

15. Managing reports of online safety incidents

15.1. Staff members and students are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies

15.2. Concerns regarding a staff member's online behaviour are reported to the headteacher who decides on the best course of action in line with the relevant policies, e.g. Staff Code of Conduct, Allegations of Abuse Against Staff Policy and Disciplinary Policy and Procedures.

15.3. Concerns regarding a student's online behaviour are reported to the DSL who investigates concerns with relevant staff members, e.g. the headteacher and ICT engineers.

15.4. Concerns regarding a student's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. Behaviour Policy and Child Protection and Safeguarding Policy.

15.5. Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

15.6. All online safety incidents and the school's response are recorded by the DSL.

15.7. Section 16 of this policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

16. Responding to specific online safety concerns

Cyberbullying

16.1. Cyberbullying, against both students and staff, is not tolerated.

16.2. Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

16.3. Information about the school's full response to incidents of cyberbullying can be found in the Cyberbullying Policy.

Online sexual violence and sexual harassment between children (peer-on-peer abuse)

16.4. The school recognises that peer-on-peer abuse can take place online. Examples include the following:

- Non-consensual sharing of sexual images and videos
- Sexualised cyberbullying

- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

16.5. The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment.

16.6. Concerns regarding online peer-on-peer abuse are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.

16.7. Information about the school's full response to incidents of online peer-on-peer abuse can be found in the Child Protection and Safeguarding Policy.

Upskirting

16.8. Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.

16.9. A "specified purpose" is namely:

- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
- To humiliate, distress or alarm the victim.

16.10. "Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

16.11. Upskirting is not tolerated by the school.

16.12. Incidents of upskirting are reported to the DSL who will then decide on the next steps to take, which may include police involvement, in line with the Child Protection and Safeguarding Policy.

Youth produced sexual imagery (sexting)

16.13. Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal.

16.14. All concerns regarding sexting are reported to the DSL.

16.15. Following a report of sexting, the following process is followed:

- The DSL holds an initial review meeting with appropriate school staff
- Subsequent interviews are held with the students involved, if appropriate
- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the student at risk of harm

- At any point in the process if there is a concern a student has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
- The interviews with staff, students and their parents are used to inform the action to be taken and the support to be implemented

16.16. When investigating a report, staff members do not view the youth produced sexual imagery unless there is a good and clear reason to do so.

16.17. If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the headteacher first.

16.18. The decision to view imagery is based on the professional judgement of the DSL and always complies with the Child Protection and Safeguarding Policy.

16.19. Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded.

16.20. If it is necessary to view the imagery, it will not be copied, printed or shared.

16.21. Viewing and deleting imagery is carried out in line with the Searching, Screening and Confiscation Policy.

Online abuse and exploitation

16.22. Through the online safety curriculum, students are taught about how to recognise online abuse and where they can go for support if they experience it.

16.23. The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

16.24. All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL and dealt with in line with the Child Protection and Safeguarding Policy.

Online hate

16.25. The school does not tolerate online hate content directed towards or posted by members of the school community.

16.26. Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. Staff Code of Conduct, Anti-Bullying Policy and Adult Code of Conduct.

Online radicalisation and extremism

16.27. The school's filtering system protects students and staff from viewing extremist content.

16.28. Concerns regarding a staff member or student being radicalised online are dealt with in line with the Child Protection and Safeguarding Policy and Prevent Duty Policy.

17. Monitoring and review

17.1. The school recognises that the online world is constantly changing; therefore, the DSL, ICT engineers and the headteacher conduct half-termly light-touch reviews of this policy to evaluate its effectiveness.

17.2. The governing board, headteacher and DSL review this policy in full on an annual basis and following any online safety incidents.

17.3. The next scheduled review date for this policy is **September 2021.**

17.4. Any changes made to this policy are communicated to all members of the school community.

Appendix 1: Online harms and risks – curriculum coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum area(s): • Health education • Computing curriculum
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: • What a digital footprint is, how it develops and how it can affect students' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum area(s): • Relationships education • Health education • RSE • Computing curriculum
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive	This risk or harm is covered in the following curriculum area(s): • Relationships education

	• Misinformation and being aware that false and misleading information can be shared inadvertently • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	• Health education • RSE • Computing curriculum • Citizenship
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What students should do if they are harmed/targeted/groomed as a result of interacting with a fake website or scam email • Who students should go to for support	This risk or harm is covered in the following curriculum area(s): • Relationships education • RSE • Health education • Computing curriculum
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them	This risk or harm is covered in the following curriculum area(s): • Relationships education

	• How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	• Computing curriculum
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How students can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm is covered in the following curriculum area(s): • Relationships education • RSE • Computing curriculum
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: • That the majority of games and platforms are designed to make money – their primary driver is to encourage people to stay online for as long as possible • How notifications are used to pull users back online	This risk or harm is covered in the following curriculum area(s): • Health education • Computing curriculum
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum

Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm is covered in the following curriculum area(s): • Health education • Computing curriculum
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum area(s): • Relationships education • RSE • Health education • Computing curriculum • Citizenship
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help	This risk or harm is covered in the following curriculum area(s): • Relationships education • Health education

	• The importance of telling an adult about challenges which include threats or secrecy – 'chain letter' style challenges	
Content which incites	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	This risk or harm is covered in the following curriculum area(s): • Relationships education • RSE
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation (CSAE) and gangs (county lines). Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching students about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm is covered in the following curriculum area(s): • Relationships education • RSE

Live streaming	Live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: • What the risks of carrying out live streaming are, e.g. the potential for people to record livestreams and share the content • The importance of thinking carefully about who the audience might be and if students would be comfortable with whatever they are streaming being shared widely • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That students should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming	This risk or harm is covered in the following curriculum area(s): • Relationships education • Health education
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following: • That pornography is not an accurate portrayal of adult sexual relationships • That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour • That not all people featured in pornographic material are doing so willingly, i.e. revenge porn or people trafficked into sex work	This risk or harm is covered in the following curriculum area(s): • RSE
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following:	This risk or harm is covered in the following curriculum area(s): • Relationships education

	• That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people students do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	• RSE • Computing curriculum
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm is covered in the following curriculum area(s): • Health education
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: • How to evaluate critically what students are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for students to consider if they are actually enjoying being online or just doing it out of habit due to peer pressure or the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues	This risk or harm is covered in the following curriculum area(s): • Health education

	• That isolation and loneliness can affect students and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect/curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm is covered in the following curriculum area(s): • Relationships education
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: • Strategies for positive use • How to build a professional online profile	This risk or harm is covered in the following curriculum area(s): • RSE
Suicide, self-harm and eating disorders	Students may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for students and should take care to avoid giving instructions or methods and avoid using language, videos and images.	