

This file was cleaned of potential threats.



Online Safety Policy

Revised: September 2025



Statement of intent

This Online Safety Policy outlines the commitment of Cardinal Allen Catholic High School to safeguard members of our school community online in accordance with statutory guidance and best practice. This policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carer and visitors) 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).

Cardinal Allen Catholic High 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.

Our school aims

- To have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- To identify and support groups of pupils that are potentially at greater risk of harm online than others.
- To deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- To establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

1. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

2. Roles and responsibilities

Governors

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The body will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the headteacher and governing body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing body
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The Network manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting a member of the senior leadership team and school network manager.
- Following the correct procedures by contacting the headteacher if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Ensure that if their child uses social media on their personal devices that they meet the minimum age requirements for the individual platforms as below:

Facebook: Minimum age is **13**. Age is self-reported at sign-up.

Instagram: Minimum age is **13**. Some features are limited for users under 18.

TikTok: Minimum age is **13**. Users under 16 have restrictions on messaging and live streaming.

Snapchat: Minimum age is **13**. Certain features are limited for minors.

X: Minimum age is **13**. Some adult content is allowed, so parental guidance is advised.

YouTube: Minimum age is **13**. Children under 13 can use **YouTube Kids**.

Discord: Minimum age is **16**.

Reddit: Minimum age is **13**. Subreddit rules and content vary.

Pinterest: Minimum age is **13**. Parental consent may be required in some regions.

WhatsApp: Minimum age is **16**.

Twitch: Minimum age is **13**. Live content can vary widely, so supervision is suggested

- Parents/carers must report any harmful online content on social media directly to the service directly using their online reporting tools. Such harms include:
 - Threats
 - Impersonation
 - Bullying & Harassment
 - Self-harm or Suicide
 - Online Abuse
 - Violent Content
 - Unwanted Sexual Advances
 - Pornographic Content

If the reported content has not been dealt with after 48 hours by the social media platform, parents/carers must report this [here](#)

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

3. Teaching and learning

Why the internet and digital communications are important

- 3.1. The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
- 3.2. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- 3.3. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- 3.4. Staff model safe and responsible behaviour in their use of technology during lessons.
- 3.5. Teachers remind pupils about their responsibilities through the Pupil Acceptable Use Agreement which every pupil will sign.

Internet use will enhance learning

- 3.6. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- 3.7. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- 3.8. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- 3.9. Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate internet content

- 3.10. The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- 3.11. Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- 3.12. Pupils will be taught how to report unpleasant internet content to their teacher or the IT Technician. This can be done anonymously, or in person, and will be treated in confidence.

- 3.13. The school has a clear, progressive online safety education programme as part of the computing and LIFE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
- To STOP and THINK before they CLICK.
 - To develop a range of strategies to evaluate and verify information before accepting its accuracy.
 - To be aware that the author of a website/page may have a bias or purpose and to develop skills to recognise what that may be.
 - To know how to narrow down or refine a search.
 - To understand how search engines work and to understand that this affects the results they see at the top of the listings.
 - To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
 - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
 - To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
 - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned-on privacy settings.
 - To understand why they must not post pictures or videos of others without their permission.
 - To know not to download any files.
 - To have strategies for dealing with receipt of inappropriate materials.
 - To understand why and how some people will 'groom' young people for sexual reasons.
 - To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
 - Understand about their 'Digital Footprint' and how social media and an internet presence is now commonly used by prospective employers to assess a persons suitability for a job / position – "digital dirt sticks".
 - To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.
 - To fully understand the consequences of posting any form on online content (both positive and negative consequences.)

4. Managing internet access

Information system security

- 4.1. School ICT systems security will be reviewed regularly.
- 4.2. Virus protection will be updated regularly.

Email

- 4.3. Pupils may only use approved email accounts on the school system.
- 4.4. Pupils must immediately tell a teacher if they receive an offensive email.
- 4.5. In email communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.
- 4.6. Incoming emails will be treated as suspicious and attachments not opened unless the author is known.
- 4.7. The school will consider how emails from pupils to external bodies are presented and controlled.
- 4.8. The forwarding of chain letters is not permitted.
- 4.9. The school:
 - Provides staff with an email account for their professional use (Microsoft 365) and makes clear personal emails should be through a separate account.
 - Does not publish personal email addresses of pupils or staff on the school website.
 - Will contact the police if one of our staff or pupils receives an email that it considers is particularly disturbing or breaks the law.
 - Will ensure that email accounts are maintained and up-to-date.
 - Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.
 - Knows that spam, phishing and virus attachments can make emails dangerous.

Published content and the school website

- 4.10. Staff or pupil personal contact information will not be published.
- 4.11. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.
- 4.12. Uploading of information is restricted to our website authorisers.
- 4.13. The school website complies with statutory DfE guidelines for publications.
- 4.14. Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- 4.15. The point of contact on the website is the school address and telephone number. The school uses a general email contact address, head@cardinalallen.co.uk. Home information or individual email identities will not be published.
- 4.16. Photographs published on the web do not have full names attached.
- 4.17. The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- 4.18. The school expects teachers using school approved blogs or wikis to password protect them and run from the school website.

Publishing pupils' images and work

- 4.19. Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.
- 4.20. Pupil image file names will not refer to the pupil by name.
- 4.21. Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- 4.22. The school gains parental permission for use of digital photographs or video involving their child as part of the school agreement form each year.
- 4.23. The school does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- 4.24. Staff sign the school's Staff Acceptable Use Agreement, and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- 4.25. If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high-profile publications, the school will obtain individual parental or pupil permission for their long-term use.
- 4.26. The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- 4.27. Pupils are taught about how images can be manipulated in their online safety education programme and to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computer Science and LIFE (PSHCE) Curriculum.
- 4.28. Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- 4.29. Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. The school teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Social networking and personal publishing

- 4.30. The school will control access to social networking sites and consider how to educate pupils in their safe use.
- 4.31. Newsgroups will be blocked unless a specific use is approved.
- 4.32. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- 4.33. Pupils will be advised to use nicknames and avatars when using social networking sites.
- 4.34. Staff will be reminded of the risks of accepting parents and children as 'friends' on social networking sites, will be strongly advised not to do so, and given advice on how to 'block' children from viewing their private pages.
- 4.35. Staff will be shown how to 'block' their profile picture from being downloaded and protect their profile information.
- 4.36. Staff will be encouraged to 'untag' themselves from any inappropriate pictures that may appear on social networking sites.
- 4.37. Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open their own spaces to their pupils, but to use the school's preferred system (Synergy) for such communications.
- 4.38. School staff will ensure that in private use:
 - No reference should be made in social media to pupils, parents or school staff.

- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or LA.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Managing filtering

- 4.39. If staff or pupils come across unsuitable online materials, the site must be reported to the IT Technician or their teacher.
- 4.40. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing and webcam use

- 4.41. Videoconferencing should use the educational broadband network to ensure quality of service and security.
- 4.42. Videoconferencing and webcam use will be appropriately supervised.

Managing emerging technologies

- 4.43. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- 4.44. The SLT should note that technologies, such as mobile phones with wireless internet access, can bypass school filtering systems and present a new route to undesirable material and communications.
- 4.45. Mobile phones will not be used during school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- 4.46. Staff will not use personal mobile phones to communicate with children or use them to capture images of them.

Protecting personal data

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

Personal devices and mobile phones

- 4.48. The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded.
- 4.49. The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.
- 4.50. Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf or seek specific permissions to use their phone at other than their break times. Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- 4.51. Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or on silent at all times.
- 4.52. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- 4.53. No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- 4.54. Any permitted images or files taken in school by staff must be downloaded from the device and deleted in school before the end of the day.
- 4.55. Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- 4.56. Staff will be issued with a school phone where contact with pupils' parents is required beyond the school day.
- 4.57. Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods, unless permission has been granted by a member of the SLT in emergency circumstances.
- 4.58. If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, it will only take place when approved by the SLT.

- 4.59. Staff will not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- 4.60. If a member of staff breaches the school policy, disciplinary action may be taken.
- 4.61. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- 4.62. Pupils will abide by the following rules when using personal devices in school:
 - The school strongly advises that pupil mobile phones should not be brought into school; however, we accept that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety.
 - If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents in accordance with the school policy.
 - If a pupil needs to contact their parents, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
 - Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in the safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Artificial intelligence (AI)

- 4.63. Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. The school recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.
- 4.64. The school will treat any use of AI to bully pupils very seriously, in line with our behaviour policy.
- 4.65. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

5. Policy decisions

Authorising internet access

- 5.1. All staff will read and sign the [Staff Acceptable Use Agreement](#) before using any school ICT resource.
- 5.2. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- 5.3. Any person not directly employed by the school will be asked to sign the [Staff Acceptable Use Agreement](#) before being allowed to access the internet from the school site.

Assessing risks

- 5.4. The school will take all reasonable precautions to prevent access to inappropriate material; however, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the LA can accept liability for any material accessed, or any consequences of internet access.
- 5.5. The school should audit ICT use to establish if the online safety Policy is adequate and that the implementation of the online safety Policy is appropriate and effective.

Handling online-safety complaints

- 5.6. Complaints of internet misuse will be dealt with by a senior member of staff.
- 5.7. Any complaint about staff misuse must be referred to the headteacher.
- 5.8. Complaints of a child protection nature must be dealt with in accordance with school [child protection procedures](#).
- 5.9. Pupils and parents will be informed of the complaints procedure (see school's complaints policy)
- 5.10. Pupils and parents will be informed of the consequences for pupils misusing the internet.
- 5.11. Discussions will be held with the police youth crime reduction officer to establish procedures for handling potentially illegal issues.

6. Pupil online safety curriculum

Teaching and learning

- 6.1. This school has a clear, progressive online safety education programme as part of the computing and LIFE curriculum. This covers a range of skills and behaviours appropriate to the age of the children.

- 6.2. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- 6.3. The school will remind pupils about their responsibilities through a [Pupil Acceptable Use Agreement](#) which every pupil will sign.
- 6.4. All staff will model safe and responsible behaviour in their own use of technology during lessons.

Online risks

- 6.5. The school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in life) that some adults and young people will use such outlets to harm children.

Cyber bullying and abuse

- 6.6. Cyber bullying can be defined as “Any form of bullying which takes place online or through smartphones and tablets.”
- BullyingUK
- 6.7. Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.
- 6.8. Through the LIFE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.
- 6.9. Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying and confiscation procedures. Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school’s policy on anti-bullying and behaviour.
- 6.10. There are clear procedures in place to support anyone in the school community affected by cyber bullying.
- 6.11. All incidents of cyber bullying reported to the school will be recorded.

Sexual exploitation/sexting

- 6.12. Sexting between pupils will be managed through our anti-bullying and confiscation procedures.
- 6.13. All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.
- 6.14. There are clear procedures in place to support anyone in the school community affected by sexting.
- 6.15. All incidents of sexting reported to the school will be recorded.

Radicalisation or extremism

- 6.16. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.
- 6.17. Extremism is the promotion or advancement of an ideology based on violence, hatred or intolerance, that aims to: negate or destroy the fundamental rights and freedoms of others; or undermine, overturn or replace the UK’s system of liberal parliamentary democracy and democratic rights ; or intentionally create a permissive environment for others to achieve the results in (1) or (2).
- 6.18. The school understands that there is no such thing as a “typical extremist”: those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.
- 6.19. The school understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff can recognise those vulnerabilities.
- 6.20. Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.
- 6.21. The school will monitor its curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.
- 6.22. Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

7. Communications policy

Introducing the online safety Policy to pupils

- 7.1. Online safety rules and guidance posters will be displayed in school and discussed with pupils regularly.
- 7.2. Pupils will be informed that network and internet use will be monitored and appropriately followed up.

- 7.3. Safety training will be embedded within the computing and LIFE programs of learning in line with national curriculum expectations.

Staff and the Online safety policy

- 7.4. All staff will be given the school online safety Policy and have its importance explained.
- 7.5. Staff must be informed that network and internet traffic can be monitored and traced to the individual user.
- 7.6. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- 7.7. Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' support

- Parents' attention will be drawn to the school online safety policy via our school newsletters, the school brochure, and on the school website.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

8. How the school will respond to issues of misuse

Staff and the Online safety policy

- 8.1. Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT acceptable use policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
- 8.2. Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- 8.3. The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

