Cardinal Allen Catholic High School

E-Safety Policy and Procedure

Revised: January 2019

Statement of intent

Our children will not only be working online in school or at home; their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

E-safety is a child protection issue, and indeed it should not be managed primarily by the ICT team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying.

An E-safety Policy should:

- Allow young people to develop their own protection strategies for when adult supervision and technological protection are not available.
- Give information on where to seek help and how to report incidents.
- Help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online.
- Provide guidelines for parents and others on safe practice.
- Ensure you regularly monitor and review your policies with stakeholders.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.

Above all, e-safety education should be a continuing feature of both staff development and young people's educational lifelong learning.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at school with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of the school.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupil.

1. Teaching and learning

Why the internet and digital communications are important

1.1. 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.

1.2. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.3. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

1.4. Staff model safe and responsible behaviour in their use of technology during lessons.

1.5. Teachers remind pupils about their responsibilities through the Pupil Acceptable Use Agreement which every pupil will sign.

Internet use will enhance learning

1.6. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

1.7. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

1.8. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

1.9. Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate internet content

1.10. The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

1.11. Pupils will be taught the importance of cross-checking information before accepting its accuracy.

1.12. 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.

1.13. The school has a clear, progressive online safety education programme as part of the computing/PSHE 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.

- 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.

2. Managing internet access

Information system security

2.1. School ICT systems security will be reviewed regularly.
2.2. Virus protection will be updated regularly.

Email

2.3. Pupils may only use approved email accounts on the school system.
2.4. Pupils must immediately tell a teacher if they receive an offensive email.
2.5. In email communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.
2.6. Incoming emails will be treated as suspicious and attachments not opened unless the author is known.
2.7. The school will consider how emails from pupils to external bodies are presented and controlled.
2.8. The forwarding of chain letters is not permitted.
2.9. 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

2.10. Staff or pupil personal contact information will not be published.
2.11. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.
2.12. Uploading of information is restricted to our website authorisers.
2.13. The school website complies with statutory DfE guidelines for publications.
2.14. 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.
2.15. 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.
2.16. Photographs published on the web do not have full names attached.
2.17. The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
2.18. 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

2.19. Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.
2.20. Pupil image file names will not refer to the pupil by name.
2.21. Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.22. The school gains parental permission for use of digital photographs or video involving their child as part of the school agreement form each year.
2.23. 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.
2.24. 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.
2.25. 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.
2.26. The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.
2.27. Pupils are taught about how images can be manipulated in their e-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 ICT scheme of work.
2.28. 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.
2.29. 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

2.30. The school will control access to social networking sites and consider how to educate pupils in their safe use.
2.31. Newsgroups will be blocked unless a specific use is approved.
2.32. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
2.33. Pupils will be advised to use nicknames and avatars when using social networking sites.
2.34. 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.
2.35. Staff will be shown how to 'block' their profile picture from being downloaded and protect their profile information.
2.36. Staff will be encouraged to 'untag' themselves from any inappropriate pictures that may appear on social networking sites.
2.37. 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 for such communications.
2.38. 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

2.39. If staff or pupils come across unsuitable online materials, the site must be reported to the IT Technician or their teacher.
2.40. 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

2.41. Videoconferencing should use the educational broadband network to ensure quality of service and security.

2.42. Videoconferencing and webcam use will be appropriately supervised.

Managing emerging technologies

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

2.44. 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.

2.45. 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.

2.46. Staff will not use personal mobile phones to communicate with children or use them to capture images of them.

Protecting personal data

2.47. 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

2.48. 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.

2.49. 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.

2.50. 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.

2.51. 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.

2.52. 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.

2.53. 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.

2.54. 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.

2.55. 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.

2.56. Staff will be issued with a school phone where contact with pupils' parents is required beyond the school day.

2.57. 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.

2.58. 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.

2.59. 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.

2.60. If a member of staff breaches the school policy, disciplinary action may be taken.

2.61. 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.

2.62. 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.

3. Policy decisions

Authorising internet access

3.1. All staff will read and sign the Staff Acceptable Use Agreement before using any school ICT resource.

3.2. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

3.3. 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

3.4. 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.

3.5. The school should audit ICT use to establish if the E-safety Policy is adequate and that the implementation of the E-safety Policy is appropriate and effective.

Handling e-safety complaints

3.6. Complaints of internet misuse will be dealt with by a senior member of staff.

3.7. Any complaint about staff misuse must be referred to the headteacher.

3.8. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

3.9. Pupils and parents will be informed of the complaints procedure (see school's complaints policy)

3.10. Pupils and parents will be informed of the consequences for pupils misusing the internet.

3.11. Discussions will be held with the police youth crime reduction officer to establish procedures for handling potentially illegal issues.

4. Pupil online safety curriculum

Teaching and learning

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

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

Online risks

4.5. 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 PSHE) that some adults and young people will use such outlets to harm children.

Cyber bullying and abuse

4.6. Cyber bullying can be defined as "Any form of bullying which takes place online or through smartphones and tablets." - BullyingUK
4.7. 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.
4.8. Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.
4.9. 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.
4.10. There are clear procedures in place to support anyone in the school community affected by cyber bullying.
4.11. All incidents of cyber bullying reported to the school will be recorded.

Sexual exploitation/sexting

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

Radicalisation or extremism

4.16. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.
4.17. Extremism is defined by the Crown Prosecution Service as "The demonstration of unacceptable behaviour by using any means or medium to express views which:
- Encourage, justify or glorify terrorist violence in furtherance of beliefs.
- Seek to provoke others to terrorist acts.
- Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
- Foster hatred which might lead to inter-community violence in the UK."

4.18. The school understands that here 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.
4.19. 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.
4.20. Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.

4.21. The school will monitor its RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.

4.22. Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

5. Communications policy

Introducing the E-safety Policy to pupils

5.1. E-safety rules and guidance posers will be displayed in school and discussed with pupils regularly.

5.2. Pupils will be informed that network and internet use will be monitored and appropriately followed up.

5.3. Safety training will be embedded within the computing and PSHE schemes of work in line with national curriculum expectations.

Staff and the e-safety policy

5.4. All staff will be given the school E-safety Policy and have its importance explained.

5.5. Staff must be informed that network and internet traffic can be monitored and traced to the individual user.

5.6. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

5.7. 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 E-safety Policy in an e-safety leaflet, 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.