Denewood
ACADEMY

Academy Policy

Online Safety Policy

CEO approval:	Sean Kelly	
LGB Cluster ratification		
Last reviewed on:	January 2026	
Next review due by:	January 2027	

Contents

1. Introduction

1.1 At Denewood Academy we take online safety very seriously to ensure the safety of our children and all staff. This policy outlines our procedures regarding online safety.

2. Policy Development

2.1 This policy has been written in full consultation with the staff, parents/carers, governors and pupils of Denewood Academy.

2.2 It has been approved by our Senior Leadership Team and governors.

2.3 The policy will be reviewed annually and is available on our school website or from the school office.

3. Role and responsibilities

3.1 The school has a

3.2 member of the Senior Leadership Team and DSL responsible for Online Safety is Emma Thornton. It is the responsibility of all adults and pupils linked to Denewood Academy to ensure that this policy is implemented fully.

4. The 4 categories of risk

4.1 As a school, we are aware that online safety has a considerable breadth of issues, which fall under the following areas of risk:

a) Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalization, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

b) Contact: being subjected to harmful online interaction with other users, for example: 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.

c) Conduct: personal online behaviour that increases the likelihood or, or causes, harm, for example, 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.

d) Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. We are aware that if we feel that our pupils, students or staff are at risk, we must report it to the Anti-Phishing Working Group (https://apwg.org/)

5. Why internet and digital communications are important to teaching and learning

5.1 The purpose of technology in school is to raise educational standards, to promote achievement, to support professional work of staff and to enhance the school's management functions.

5.2 Denewood Academy has a duty to provide pupils with quality internet access as part of their learning experience

5.3 Internet use is part of the statutory curriculum and a necessary tool for staff

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

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

5.6 Pupils will be taught what internet use is acceptable, and what is not, and be given clear objectives for use. These are also important transferrable skills for their life out of school, including with the use of mobile phones and other mobile devices.

5.7 Pupils will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact.

5.8 We include issues such as Cyberbullying and e-safety in our curriculum to encourage self-efficacy and resilience. We ensure we support all children where necessary.

6. Managing internet access

6.1 The school's ICT system security is reviewed regularly, and our virus protection is regularly updated.

7. Cyber Security

7.1 Flywheel, our IT support company, ensure the appropriate level of security protection procedures are in place to safeguard internal systems. These are reviewed periodically to ensure their effectiveness and keep up with evolving cyber-crime technologies.

8. Filtering and monitoring

8.1 To safeguard and promote the welfare of children at our school and provide them with a safe environment in which to earn, we limit children's exposure through, filtering and monitoring on school devices and school networks. The filtering and monitoring company we use is Smoothwall. Regular reviews take place to identify their effectiveness. The Senior Leadership Team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

8.2 Denewood Academy has identified and assigned roles and responsibilities to manage filtering and monitoring systems:

a) Review filtering and monitoring provision at least annually

b) Block harmful and inappropriate content without unreasonably impacting teaching and learning needs

c) Have effective monitoring strategies in place that meet safeguarding needs

8.3 Parental communications to reinforce the importance of children being safe online is provided to understand what systems the school use to filter and monitor online use. The importance for parents and carers to be aware of what their children are being asked to do online is taken into account, including the sites they will be asked to access and who their child will be interacting with.

8.4 All staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of their safeguarding training and how to report safeguarding and technical concerns.

8.5 The school has additional policies that support / identify filtering and monitoring.

9. Published content and the school website

9.1 The contact details on the school's website are the school address and phone number; no staff or pupil's personal details will be published.

9.2 The Head of School has overall editorial responsibility of the website to ensure that content is accurate and appropriate.

10. Publishing Pupils' images and work

10.1 Photographs that include identifiable images of children should only be added to the school's website and Class Dojo with consent from the parent/carer.

10.2 Pupil's full names will be avoided on the website, especially with associated photographs.

10.3 Parents are informed about our school policy on image taking and publishing.

11. Class Dojo

11.1 Class Dojo is used as Denewood Academy's main means of communication with parents/carers.

11.2 Staff may reply to messages sent by parents on Class Dojo but the expectation is that this is not done after 5pm.

11.3 Relevant online safety information is shared with parents via Class Dojo.

12. Social Networking

12.1 The school does not allow use of any social network sites for children.

13. Mobile Phones

13.1 Any mobile phones brought into school, are required to be handed to the class teacher and returned at the end of the day.

13.2 The school recognises youth produced sexual imagery, sharing of nude and semi-nude images (previously known as "sexting") as a safeguarding issue; all concerns should be reported to and dealt with by the Designated Safeguarding Lead (DSL) in line with the academy's Safeguarding and Child Protection policy.

13.3 The school recognises the need for children to be kept safe from terrorist and extremist material; therefore, it will be covered by the e-safety curriculum.

14. Video Conferencing

14.1 Any video conferencing is supervised

14.2 Any video conferencing will use the educational broadband network to ensure quality of service and security.

15. Managing Emerging Technologies

15.1 The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.

15.2 Mobile phones and associated cameras will not be used in lessons or school time as part of an educational activity.

15.3 Care will be taken with the use of hand-held technologies in school which may not have the level of filtering required.

15.4 In the event of staff working from home, 141 must be used before any phone calls are made

16. Artificial intelligence (AI)

15. 1 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.

15.2 The academy recognises that AI has many uses, including enhancing teaching and learning, and in helping to protect and safeguard pupils. However, AI may also have the potential to facilitate abuse (e.g. bullying and grooming) and/or expose pupils to harmful content. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

15.3 Staff will treat any use of AI to access harmful content or bully pupils in line with the Safeguarding and Child Protection policy and Relationships and Positive Behaviour policy.

15.4 Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out risk assessments for any new AI tool being used by the academy.

17. Network Management (user access, back up)

17.1 The school uses individual, audited log-ins for all staff users.

17.2 Storage of all data within the school will conform to the UK data protection requirements and subsequent General Data Protection Regulation (GDPR).

18. Policy Decisions

18.1 Assessing risks

18.1.1 The school will take reasonable precautions to prevent access to inappropriate material; however, it is not possible to guarantee that unsuitable material will never appear on a school ICT resource.

18.1.2 The school will monitor ICT use to establish if the Online Safety policy is appropriate and effective.

19. Arrangements for Reporting Online Safety Incidents

19.1 Raising concerns regarding radicalisation

19.1.1 Our Designated Safeguarding Lead (DSL) provides advice and support to other members of staff on protecting children from the risk of on-line radicalisation. Denewood Academy ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify children at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism.

19.1.2 Staff safeguard and promote the welfare of children and know where and how to refer children and young people for further help as appropriate by making referrals as necessary to Channel.

19.2 Inside School

19.2.1 Any incident must be reported to the Designated Safeguarding Lead and logged on CPOMS.

19.2.2 If available, any evidence must be kept.

19.2.3 Statements must be taken from all parties.

19.2.4 A member of the Senior Leadership Team must be informed and decide on the best course of action – this may include school-based sanctions, meetings with parents and, in the most severe incidents, the PCSOs and Police may be involved.

19.2.5 All incidents must be recorded on CPOMS.

19.3 Outside School

19.3.1 As soon as a member of staff is made aware of any online safety incident, they must follow the guidance above.

19.3.2 Parents should always be informed when online safety incidents occur outside of school and given appropriate support where necessary.

19.3.3 Children are regularly reminded of how to keep safe online and if any incidents were to occur, what they must do. They are also made aware of CEOP www.ceop.police.uk and Childline www.childline.org.uk 0800 1111.

20. Handling Online Safety Complaints

20.1 Complaints of internet misuse will be dealt with by the Head of school.

20.2 Complaints of misuse by staff will also be dealt with by the Head of School.

20.3 Any complaints of a child protection nature will be dealt with in accordance with child protection procedures.

20.4 Pupils and parents will be informed of the consequences and sanctions for pupils missing the internet and it will be in line with the behaviour policy.

21. Communicating our Policy

21.1 Pupils

21.1.1 Appropriate sections of this policy will be shared with pupils

21.1.2 Online safety rules will be visible around school and pupils will be involved with the development of these.

21.1.3 Age-appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified.

21.2 Staff

21.2.1 All staff will be given a copy of the Online Safety policy and will sign the Acceptable Use policy.

21.2.2 Staff will be made aware that the system is monitored and that professional standards are expected.

21.2.3 New staff have online checks carried out as part of our recruitment process.

21.3 Parents

21.3.1 Parents will be notified of the policy in newsletters and via Class Dojo.

21.3.2 The academy provides learning opportunities for parents on this topic through coffee mornings, online safety events and signposting to useful resources.