Ambleside ACADEMY

Academy Policy

E-safety Policy

CEO approval:	Sean Kelly	
LGB Cluster ratification	Mainstream Cluster	
Last reviewed on:	September 2023	
Next review due by:	September 2024	

Contents

1. Policy development

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

1.2 It has been approved by our senior Leadership Team and governors.

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

2. Roles and responsibilities

2.1 The school has a computing lead in class teacher Holly Hutchinson and the member of the Senior Leadership Teams and DSL responsible for E Safety is Louise Marsh. It is the responsibility of all adults and pupils linked to Ambleside Academy to ensure that this policy is implemented fully.

3. Online safety

3.1 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, radicalisation, and extremism.

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 behavior 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/)

4. Why internet and digital communications are important

4.1 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.

4.2 Ambleside Academy has a duty to provide students with quality internet access as part of their learning experience

4.3 Year 5 and 6 students are provided with an iPad each to support their learning within the classroom. With parental consent, this iPad can also be taken home to support with homework and other learning at home.

4.4 Internet use is part of the statutory curriculum and a necessary too for staff

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

4.6 Students will be shown how to publish and present information appropriately to a wider audience.

4.7 Students 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.

4.8 Students will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact.

4.9 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.

5. Managing internet access

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

6. Filtering and Monitoring

6.1 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, monitoring and filtering on school devices and school networks. The monitoring and filtering 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. The company we use is Consideration is taken into account to the number of and age range of children in the school.

6.2 Ambleside 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

We have employed Flywheel as out IT support company.

6.3 The LGFL Online Safety Audit is completed annually by the DSL – Louise Marsh – and then shared with the rest of the DSL team.

6.4 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.

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

7. Email

7.1 All in-coming emails should be treated as suspicious and attachments should not be opened unless the author is known.

7.2 The forwarding of chain letters is not permitted

8. Published content and the school website

8.1 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.

8.2 The Principal has overall editorial responsibility of the website to ensure that content is accurate and appropriate.

9. Publishing pupils' images and work

9.1 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.

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

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

10. Class Dojo

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

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

10.3 Relevant e-safety information is shared with parents via Class Dojo.

11. Social networking

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

11.2 The school uses Purple Mash to set out-of-school activities which are private and controlled.

12. Mobile phones

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

12.2 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).

12.3 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.

13. Video conferencing

13.1 Any video conferencing is supervised

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

14. Managing emerging technologies

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

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

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

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

15. Network management (user access, back up)

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

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

16. Protecting personal data

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

17. Assessing risks

17.1 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.

17.2 The school will monitor ICT use to establish if the e-safety policy is appropriate and effective.

18. Arrangements for reporting e-safety incidents

18.1 Raising concerns regarding radicalisation

a) Our Designated Safeguarding Lead provides advice and support to other members of staff on protecting children from the risk of on-line radicalisation. Ambleside Academy ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism.

b) 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 legitimist terrorism. 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.

18.2 Inside school

a) Any incident must be reported to a child's class teacher as soon as possible.

b) If available, any evidence must be kept.

c) Statements must be taken from all parties.

d) 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.

e) All incidents must be recorded and logged.

18.3 Outside of school

a) As soon as a member of staff is may aware of any e-safety incident, they must follow the guidance above.

b) Parents should always be informed when e-safety incidents occur outside of school.

c) 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.

18.4 Handling e-safety complaints

a) Complaints of internet misuse will be dealt with by the Principal.

b) Complaints of misuse by staff will also be dealt with by the Principal.

c) Any complaints of a child protection nature will be dealt with in accordance to child protection procedures.

d) 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.

19. Communicating our Policy

19.1 Pupils

a) Appropriate sections of this policy will be shared with pupils

b) E-safety rules will be visible around school and pupils will be involved with the development of these.

c) 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.

19.2 Staff

a) All staff will be given a copy of the e-safety policy and will sign the acceptable use policy.

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

c) In line with KICSIE 20223 new staff have online checks carried out as part of our recruitment process.

19.3 Parents

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