Ashingdon Primary Academy
Academies Enterprise Trust

e-safety policy
September 2021

Reviewed : January 2022

One AET. Safer lives; greater learning.

Further advice and guidance relating to this policy can be obtained from Rowena Simmons, Trust

Designated Safeguarding Lead: rsimmons@academiesenterprisetrust.org

Contents

1. Our commitment

1.1. The Academies Enterprise Trust (AET*)* is committed to bringing our academies and school support services together to work as one AET and to ensure safer lives and greater learning for all children and young people.As we increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material.

1.2. The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. Please see Appendix 1: Online safeguarding issues

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

a) **content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
b) **contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
c) **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

1.4 Accordingly, we have appropriate internet filtering within our academy and our central support services and we utilise eSafe to monitor all activity within our AET Google suite of applications; in particular the content of information, the nature of the contact and the conduct of the user. The welfare and safety of each individual child is paramount and therefore we are committed to providing a safe online learning environment by:

a) Ensuring robust processes are in place to ensure the online safety of pupils, staff, volunteers and governors.
b) Delivering an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
c) Establishing clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and guidance

2.1. This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education 2021 and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's Prevent guidance on protecting children from radicalisation.

2.2. This policy 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.

2.3. This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1. The AET Board of Trustees

The Board of Trustees delegates responsibility for ratifying the e safety policy at each review to the Executive Committee.

3.2. The Local Governing Board (LGB)

3.2.1 The LGB has overall responsibility for monitoring this policy and holding the headteacher/ principal to account for its implementation.

3.2.2 The LGB will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs/electronic records as provided by the academy designated safeguarding lead (DSL). The governor who oversees online safety is named within our website governor information page.

3.2.3 All governors will:

a) Ensure that they have read and understood this policy
b) Sign to confirm they agree and will adhere to the terms on acceptable use as detailed in the AET e-safety charter for staff .

c) Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 76) and the requirement 112 The Prevent duty Departmental advice for schools and childcare providers and Prevent Duty Guidance For Further Education Institutions to ensure children are taught about safeguarding, including online (paragraph 80), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

3.3. The Headteacher/Principal

The academy headteacher/principal is responsible for:

a) ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
b) ensuring that all staff sign to agree and adhere to the APA e-safety charter for staff
c) monitoring incident reports produced by eSafe and taking appropriate action if necessary.

3.4. The academy Designated Safeguarding Lead

Details of the academy's designated safeguarding lead (DSL) are set out in our Safeguarding and Child Protection Policy. The DSL takes lead responsibility for online safety in school, in particular:

a) Supporting the headteacher/principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
b) Working with the headteacher, IT manager and other staff, as necessary, to address any online safety issues or incidents
c) Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
d) Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
e) Updating and delivering staff training on online safety
f) Liaising with other agencies and/or external services if necessary
g) Providing regular reports on online safety in school to the headteacher and/or governing board
h) Monitoring eSafe incident reports, where designated to do so and taking appropriate action.

3.5. The academy IT manager/lead

The IT manager/lead is responsible for:

a) Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful

and inappropriate content and contact online while at school, including terrorist and extremist material. This includes the implementation and maintenance of the eSafe system.

b) Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
c) Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
d) Ensuring that any online safety incidents are recorded and dealt with appropriately in line with this policy
e) Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school behaviour policy

3.6. All staff and volunteers

All staff, including contractors and agency staff, and volunteers will be vigilant to ensure the safe use of online technology and be particularly aware of pupils who may be more vulnerable, e.g. SEND pupils, pupils who are at risk of radicalisation as detailed in section 5 of our Safeguarding and Child Protection Policy. Staff are responsible for:

a) Maintaining an understanding of this policy
b) Implementing this policy consistently
c) Signing to show their agreement and intention to adhere to the terms on the AET's e-safety charter for staff and ensuring that pupils follow the academy's terms on acceptable use
d) Working with the DSL to ensure that any online safety incidents are recorded and dealt with appropriately in line with this policy
e) Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school behaviour policy

3.7. The Trust Designated Safeguarding Lead (DSL)and deputy DSL

The Trust DSL will support academy DSLs by:

a) Providing opportunities to share best practice with each other at regional and national conference and with other organisations, e.g. NSPCC
b) Providing regular updates and resources through the Google+ community and the AET safeguarding portal.
c) Providing support and guidance on specific matters relating to online safety as appropriate.

3.8. Parents

3.8.1 Parents are expected to:

a) Notify a member of staff or the headteacher of any concerns or queries regarding this policy
b) Ensure their child has read, understood and agreed to the terms on acceptable use of the academy's IT systems and internet

3.8.2 Parents can seek further guidance on keeping children safe online from the following organisations and websites:

a) What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
b) Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
c) Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.9. Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use, see Appendix 2 AET e-safety charter for staff.

4. Educating pupils about online safety

4.1. Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

a) Use technology safely and respectfully, keeping personal information private
b) Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In **Key Stage 2**, pupils will be taught to:

a) Use technology safely, respectfully and responsibly
b) Recognise acceptable and unacceptable behaviour
c) Identify a range of ways to report concerns about content and contact

4.2. The safe use of social media and the internet will also be covered in other subjects where relevant for example PSHE.

4.3. The academy will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

5.1. The academy will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents on our website.

5.2. Online safety will also be covered during parents' evenings.

5.3. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

5.4. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyberbullying

6.1. Definition

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the academy behaviour policy.)

6.2. Preventing and addressing cyber-bullying

6.2.1 To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victims.

6.2.2 The academy will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes when appropriate, and the issue will be addressed in assemblies.

6.2.3 Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

6.2.4 All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

6.2.5 The academy also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

6.2.6 In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

6.2.7 The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.2.8 See also Appendix 1: Online safeguarding issues for information relating to other online safeguarding issues.

6.3. Examining electronic devices

6.3.1 Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

6.3.2 When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

a) Cause harm, and/or
b) Disrupt teaching, and/or
c) Break any of the school rules

6.3.4 If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

a) Delete that material, or
b) Retain it as evidence (of a criminal offence or a breach of school discipline
c) Report it to the police

6.3.5 Any searching of pupils must be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

6.3.6 Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in the academy

7.1. All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the academy's IT systems and the internet (Appendix 2 AET e-safety charter for staff). Visitors will be expected to read and agree to the academy's terms on acceptable use if relevant.

7.2. Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

7.3. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

7.4. More information is set out in the e-safety charter agreements in appendix 2 AET e-safety charter for staff.

8. Pupils using mobile devices in the academy

8.1. Pupils may bring mobile devices into the academy, Pupils may bring mobile devices into the academy these must be handed to staff for safe keeping for the entire school day. Pupils are not permitted to use them during:

a) Lessons or assemblies or any other educational activity
b) Clubs before or after school, or any other activities organised by the academy.

8.2. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement, particularly those devices with 3G and 4G access

8.3. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the academy behaviour policy, which may result in the confiscation of their device.

8.4. When pupils are working within the AET Google suite of applications on laptops or home computers outside of the academy, their activity will still be subject to eSafe monitoring. This does not apply to mobile phones, iPads and Mac computers.

9. Staff using work devices outside of the academy

9.1. Staff members using a work device outside of the academy must not install any unauthorised software on the device and must not use the device in any way which would violate the academy's terms of acceptable use, as set out in the AET e-safety charter for staff

9.2. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside of the academy. Any USB devices containing data relating to the school must be encrypted.

9.3. When staff are working on work devices outside of the academy and within the AET Google suite of applications, their activity will still be subject to eSafe monitoring.

10. How the academy will respond to issues of misuse

10.1 Where a pupil misuses the academy's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

10.2 Where a staff member misuses the academy's IT 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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

10.3 The academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

11.1 All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

11.2 All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

11.3 The academy DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

11.4 Local governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

11.5 Volunteers will receive appropriate training and updates, if applicable.

11.6 More information about safeguarding training is set out in our safeguarding and child protection policy.

12. Monitoring arrangements

The DSL (and deputy/deputies)) monitor behaviour and safeguarding issues related to online safety including any monitoring notifications from eSafe.