e-Safety Policy

November 2018

Signed (Chair of Trustees):	
Date:	November 2018
Date of Review:	November 2019

The Arbor Academy Trust reviews this policy annually. The Trustees may, however, review the policy earlier than this, if the Government introduces new regulations, or if the Trust receives recommendations on how the policy might be improved. This document is also available in other formats e.g. e-mail and enlarged print version, on request to the School Offices and is displayed on the schools' websites.

1. Introduction

1.1. The e-safety policy for the Trust advocates the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity.

1.2. The e-Safety Policy is part of the Trust's Development Plan and relates to other policies including those for computing, bullying and for child protection.

1.3. The Trust has an appointed e-Safety Coordinator who is also the computing coordinator.

2. Teaching and Learning

2.1. The Internet is an essential element in 21st century life for education, business and social interaction. The Trust has a duty to provide pupils with quality internet access as part of their learning experience.

2.2. The Trust's internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

2.3. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

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

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

2.6. The Trust will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

2.7. Pupils will be taught how to report unpleasant Internet content.

2.8. Pupils will be made aware of appropriate internet use.

3. Managing Internet Access

3.1. The Trust's computing systems security will be reviewed regularly.

3.2. Virus protection will be updated regularly.

4. E-mail

4.1. Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail.

4.2. In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

4.3. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

4.4. The forwarding of chain letters is not permitted.

5. The School Website

5.1 Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.

5.2 The CEO will take overall editorial responsibility and ensure that content is accurate and appropriate.

6. Publishing Pupil's Images and Work

6.1 Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children.

6.2 Pupils' full names will not be used anywhere on a school Website or other on-line space, particularly in association with photographs.

6.3 Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.

6.4 Work can only be published with the permission of the pupil and parents/carers.

6.5 Pupil image file names will not refer to the pupil by name.

6.6 Parents should be clearly informed of The Trust's policy on image taking and publishing, both on Trust and independent electronic repositories.

7. Social Networking

7.1 The Trust will control access to social networking sites and consider how to educate pupils in their safe use.

7.2 Newsgroups will be blocked unless a specific use is approved.

7.3 Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

7.4 Pupils and parents will be advised that the use of social network spaces outside the Trust brings a range of dangers for primary aged pupils and is strongly discouraged. Parents are reminded that the legal age for owning a Facebook account is thirteen.

8. Managing filtering

8.1 If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.

8.2 Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

9. Managing Video-conferencing and Webcam Use

9.1 Video-conferencing should use the educational broadband network to ensure quality of service and security.

9.2 Pupils must ask permission from the supervising teacher before making or answering a video-conference call.

9.3 Video-conferencing and webcam use will be appropriately supervised for the pupils' age.

10. Managing emerging technologies

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

10.2 The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass filtering systems and present a new route to undesirable material and communications.

10.3 Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

10.4 The use by pupils of cameras in mobile phones will be kept under review.

10.5 Staff will be issued with a school phone where contact with pupils is required or where mobile phones are used to capture photographs of pupils.

11. Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018.

12. Policy Decisions

12.1 All staff must read and sign the Staff Code of Conduct for computing before using any school computing resource.

12.2 The Trust will maintain a current record of all staff and pupils who are granted access to school computing systems.

12.3 At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific approved on-line materials.

12.4 Parents will be asked to sign a consent form as part of the home school agreement.

13. Assessing risks

13.1 The Trust 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. The Trust cannot accept liability for any material accessed, or any consequences of Internet access.

13.2 The Trust should audit computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

14. Handling e-safety complaints

14.1 Complaints of Internet misuse will be dealt with by the CEO.

14.2 Complaints of a child protection nature must be dealt with in accordance with Trust's child protection procedures.

15. Communications Policy

15.1 e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

15.2 Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

15.3 A programme of training in e-Safety will be developed. e-Safety training will be embedded within the computing scheme of work or the Personal Social and Health Education (PSHE) curriculum.

15.4 All staff will be given the e-Safety Policy and its importance explained. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

16. Enlisting Parents' and Carers' Support

16.1 Parents and carers' attention will be drawn to the Trust's e-Safety Policy in newsletters, the school brochure and on the school Web site.

16.2 The Trust will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

17. Monitoring and Review

Our e-Safety Policy has been written by the Trust and has been agreed by senior management and approved by Governors. It is revised annually and should be read in conjunction with the excellent material from Becta and CEOP.