E-Safety Policy

2016-17

E-Safety Policy

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

The DfE Core e-Safety Policy

This core e-safety policy provides the essential basic coverage and is made up of advice and current checklists created by the Department for Education.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the RM Managed service including the effective management of RM SafetyNet filtering.

1.0 E-Safety Audit.

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with DfE guidance?	Y/N
Date of latest update: tbc	
The Policy was agreed by:	
The Policy is available for staff in School Policy folder	
And for parents on request	
The Designated Child Protection Coordinator is: Lisa Miller	
The e-Safety Coordinator is: Lisa Miller	
Has e-safety training been provided for both students and staff?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Have school e-Safety Rules been set for students?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access (e.g. RM Managed Service).	Y/N
Has the school filtering policy has been approved by SMT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMT?	Y/N

2.0 School e-safety policy

2.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The school has an appointed e-Safety coordinator.
- Our e-Safety Policy has been written by the school. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was created by: Lisa Miller (Dec 2016)

2.2 Teaching and learning

2.2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2.3 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

2.2.4 Pupils will be taught how to evaluate Internet content

- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.3 Managing Internet Access

2.3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority and/or RM Managed Services

2.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

2.3.3 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified (unless prior consent has been given)
- Pupils' full names will not be used anywhere on the Web site (unless consent has been given) particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.

2.3.5 Social networking and personal publishing

- School will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must not place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

2.3.6 Managing filtering

- Arco Academy Alternative Provision will work in partnership with the LA, RM, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.7 Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

2.3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Alternative Provision is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Use of personal technologies are forbidden, this includes MP3 players.

2.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.4 <u>Policy Decisions</u>

2.4.1 Authorising Internet access

- All staff must read and sign the 'Staff Acceptable Use Policy' before using any Alternative Provision ICT resource.

- The Alternative Provision will maintain a current record of all staff and pupils who are granted access to the Alternative Provision ICT systems.
- Pupils must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.
- Parents will be asked to sign and return a consent form.

2.4.2 Assessing risks

- The Alternative Provision will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on an Alternative Provision computer. Arco Academy Alternative Provision cannot accept liability for the material accessed, or any consequences of internet access.
- The Alternative Provision should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

2.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

2.4.4 Radicalisation Procedures and Monitoring

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 particular 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

Although serious incidents involving radicalisation have not occurred at Arco Academy Alternative Provision to date, it is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach.

Staff are reminded to:

- suspend any professional disbelief that instances of radicalisation ‘could not happen here’
- refer any concerns through the appropriate channels (currently via the Child Protection/ Safeguarding Co-ordinator).

- Smoothwall filtering is in place to ensure that access to inappropriate material on the internet to ensure safety for all staff and students.
- Report any attempted access to the following: articles, videos, soundbites, blogs/vlogs, images or social media regarding radicalisation or extremism.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- e-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.

2.5.2 Staff and the e-Safety policy

- All staff will be asked to read the Alternative Provision e-Safety Policy and its importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

2.5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in any newsletters, information cards and on the school Web site.