

The logo for Arco Academy features a stylized blue swoosh above the word "arco" in a bold, lowercase sans-serif font. Below "arco", the word "ACADEMY" is written in a smaller, all-caps sans-serif font with wide letter spacing.

arco **A C A D E M Y** **Online Safety Policy**

Reviewed date: September 2026

Reviewed and approved by Proprietor/CEO: Lisa Miller

Reviewed and approved by the Advisory Board: Verena West (Chair), Sandie Quinn, (Safeguarding), Ken Adams (Education, compliance and H&S)

CONTENTS

Section 1 - Aims	3
Section 2 - Legislation and Guidance	3
Section 3 - Roles and Responsibilities	3
3.1 The Advisory Board	3
3.2 The Principal	3
3.3 The Designated Safeguarding Lead	3
3.4 The Ict Manager	4
3.5 All Staff And Volunteers	4
3.6 Parents	5
3.7 Visitors and Members of The Community	5
Section 4 - Educating Students About Online Safety	5
Section 5 - Educating Parents About Online Safety	6
Section 6 - Cyber-Bullying	6
6.1 Definition	6
6.2 Preventing and Addressing Cyber-Bullying	6
6.3 Examining Electronic Devices	7
Section 7 - Acceptable Use of The Internet in Academy	7
Section 8 - Students Using Mobile Devices in Academy	9
Section 9 - Staff Using Work Devices Outside The Academy	9
Section 10 - How The Academy Will Respond To Issues Of Misuse	10
Section 11 - Training	10
Section 12 - Monitoring Arrangements	10
Section 13 - Links With Other Policies	10
Appendix 1: KS3 And KS4 Acceptable Use Agreement (Students And Parents/Carers)	12
Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers And Visitors)	13
Appendix 3: Online Safety Training Needs – Self Audit For Staff	14
Appendix 4: Online Safety Incident Report Log	15

SECTION 1 - AIMS

Arco Academy aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole academy community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

SECTION 2 - LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying and cyber-bullying: advice for principals and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)
- [Meeting Digital and Technology Standards in Schools and Colleges](#)

It also refers to the Department's guidance on protecting children from radicalisation.

It 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 students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

SECTION 3 - ROLES AND RESPONSIBILITIES

3.1 The Advisory Board

The advisory board has overall responsibility for monitoring this policy and holding the principal to account for its implementation.

The advisory board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All board members will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the academy's ICT systems and the internet (appendix 3)

3.2 The principal

- The principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the academy. The Principal participates in the team which undertakes the formal annual review of filtering and monitoring

3.3 The designated safeguarding lead

Details of the academy's DSL and DDSL are set out in our safeguarding (child protection) policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety, including the oversight of the quality of filtering and monitoring in the academy, in particular:

- Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the academy to the principal and/or advisory board
- Participating in the team which undertakes the formal annual review of filtering and monitoring This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at the academy, including terrorist and extremist material
- Ensuring that the academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the academy's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour and anti-bullying policies
- Participating in the team which undertakes the formal annual review of filtering and monitoring This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the academy's ICT systems and the internet (appendix 3), and ensuring that students follow the academy's terms on acceptable use (appendices 1 and 2)

- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the academy's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? - [UK Safer Internet Centre](#)
- Hot topics - [Childnet International](#)
- Parent factsheet - [Childnet International](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the academy's ICT 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 (appendix 3).

SECTION 4 - EDUCATING STUDENTS ABOUT ONLINE SAFETY

Students will be taught about online safety as part of the curriculum and the wider curriculum, such as assemblies and themed occasions, for example, marking National Online Safety Week.

The academy teaches [Relationships and Sex Education and Health Education](#) with due regard to the DfE guidance. Please refer to the academy's Relationships and Sex Education Policy for further details.

The DfE guidance sets out requirements related to online safety.

In Key Stage 3, students are taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns Students in Key Stage 4 are taught:
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them

- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

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

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

SECTION 5 - EDUCATING PARENTS ABOUT ONLINE SAFETY

To enable parents to be better able to keep their children safe online at home, 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.

Online safety will also be covered during parents' evenings.

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

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

SECTION 6 - CYBER-BULLYING

6.1 Definition

Cyber-bullying 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 behaviour and anti-bullying policies.)

6.2 Preventing and addressing cyber-bullying

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

The academy will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Relationship and Sexual education (RSE), and other subjects, where appropriate.

All staff, advisory board and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

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.

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

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.

To further prevent cyberbullying or any other act of bullying via electronic devices, all iPad's have had the camera app disabled to prevent any unwanted photos of students being taken and used for bullying. As well as this, airdrop on the iPad's has also been disabled to prevent the sharing of any material that could be used to bully any students or staff at Arco Academy.

6.3 Examining electronic devices.

Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011 and the DfE guidance, 'Searching, Screening and Confiscations 2022') to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

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:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the academy rules

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:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of academy discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any image which indicates that a crime may have been committed will not be deleted until this is sanctioned by the police, since it may be needed as evidence in a future court case. For further information, please refer to the academy's policy on searching, screening and confiscation.

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

SECTION 7 - ACCEPTABLE USE OF THE INTERNET IN THE ACADEMY

All students, parents/carers, staff, volunteers and CEO & Advisory board are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the internet (appendices 1-2). Visitors will be expected to read and agree to the academy's terms on acceptable use if relevant.

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.

We will monitor the websites visited by students, staff, volunteers, advisory board and visitors (where relevant) to ensure they comply with the above.

As a default, all routers have web filters and parental control. This includes social media websites. This means that anyone with access to the school's Wi-Fi will be blocked from being able to access restricted websites. This applies to mobile phone devices, laptops and iPads.

iPads have a parental lock on them to restrict the use of apps not appropriate to the students' learning. Internet restrictions have been applied to iPad's internet apps (safari and google chrome) which blacklist any websites deemed inappropriate.

More information is set out in the acceptable use agreements in appendices 1 and 2.

SECTION 8 – FILTERING AND MONITORING OF INTERNET PROVISION

The DfE guidance, 'Digital and Technology Standards', which includes guidance on 'Filtering and Monitoring' placed additional expectations on the academy in relation to filtering and monitoring of internet provision. The academy has due regard to this guidance. Consequently, the DSL has overall responsibility for filtering and monitoring; this is a safeguarding role, not a technical role. An understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring is included in safeguarding and child protection training at induction for all new staff. All staff undertake at least annual cybersecurity training.

Filtering

Filtering is designed to block harmful content without 'overblocking' which may impact on teaching and learning or the school's administration. Students should not be prevented from undertaking genuine research, for example, about keeping safe or related to coursework. Filtering must be effective in any language used in the academy.

Monitoring

The academy seeks to have effective monitoring strategies to meet the safeguarding needs of the students.

Monitoring includes:

- Physical monitoring (ie staff presence)
- Live software viewing
- Monitoring user logs
- Individual device monitoring

Annual Review

In accordance with the DfE guidance, filtering and monitoring are formally reviewed at least annually. A review team typically comprises the CEO and/or a member of the Advisory Board, The Principal and/or a member of SLT, the DSL, the ICT manager and a representative of the IT provider. The review includes the checking of students' browsing history and is recorded and shared, as appropriate.

The roles and responsibilities of members of the academy community are as follows:

8.1 The CEO and Advisory Board:

- Ensure that either a nominated board member or the CEO is appointed to have governance oversight of filtering and monitoring
- Ensure that this nominated person and, optionally, other board members undertake cybersecurity training at least annually
- Assure themselves that filtering and monitoring procedures meet requirements and are effective

8.2 Principal and Senior Leadership Team:

- Procure effective filtering and monitoring systems
- Document decisions on what is blocked or allowed and why

- Review the effectiveness of the Academy's filtering and monitoring provision
- Oversee reports relating to filtering and monitoring

- Ensure that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns
- Work closely with the CEO and Advisory Board, the DSL and IT service providers in all aspects of filtering and monitoring.

8.3 The DSL:

- Oversee and act on
 - reports on the checking of filtering and monitoring,
 - safeguarding concerns
 - the checking of filtering and monitoring systems

8.4 The IT Service provider, (both in-house and external):

- maintain filtering and monitoring systems effectively
- provide filtering and monitoring reports
- complete actions following concerns or checks to systems
- work with the leadership team and DSL to procure systems, identify risk, carry out reviews and undertake checks

8.5 All Academy staff.

- Report if you see or suspect that unacceptable content has been accessed
- Report if, for example, during lesson planning and preparation you identify that unacceptable content can be accessed
- Report in advance if teaching content might cause a spike in filtering logs. For example, drugs education
- Report failure or abuse of the system
- Report any restrictions which are perceived to be unreasonable
- Report any abbreviations, misspellings or slang terms (particularly newly coined terms) which, when used in searches, may allow access to inappropriate content. (Sometimes such terms are deliberate created in order to bypass filtering).

SECTION 9 - STUDENTS USING MOBILE DEVICES IN ACADEMY

Students may bring mobile devices into the academy, but they are handed in at the start of the day and placed in individual wallets with names on and kept in a secure place for the day.

Any use of personal electronic devices in the academy by students must be in line with the acceptable use agreement (see appendix 1).

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

SECTION 10 - STAFF USING WORK DEVICES OUTSIDE THE ACADEMY

Staff members using a work device outside 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 appendix 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 the academy. Any USB devices containing data relating to the academy must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

SECTION 11 - HOW THE ACADEMY WILL RESPOND TO ISSUES OF MISUSE

Where a student misuses the academy's ICT systems or internet, we will follow the procedures set out in our policies on [behaviour and internet acceptable use]. The action taken will depend on the individual circumstances, the nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the academy's ICT 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/staff code of conduct]. The action taken will depend on the individual circumstances, the nature and seriousness of the specific incident.

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

SECTION 12 - TRAINING

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

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).

The DSL and DDSL 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.

Advisory Board will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding (child protection) policy.

SECTION 13 - MONITORING ARRANGEMENTS

The DSL logs behaviour and safeguarding issues related to online safety and any issues relating to filtering and monitoring. An incident report log can be found in appendix 4.

This policy will be reviewed every year by the principal. At every review, the policy will be shared with the advisory board.

SECTION 14 - LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- Safeguarding (child protection) policy
- Behaviour policy
- Anti-bullying policy



- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Internet acceptable use policy
- Searching, Screening and Confiscations Policy

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of student:

I will read and follow the rules in the acceptable use agreement policy

When I use the academy's ICT systems (like computers or laptops) and get onto the internet in the academy I will:

- Always use the academy's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a member of staff is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it **I will not:**
- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the academy's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal electronic device into the academy:**
- I will not use it during lessons, tutor group time, clubs or other activities organised by the academy, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the academy will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (student):

Date:

Parent/carer's agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for students using the academy's ICT systems and internet, and for using personal electronic devices in the academy, and will make sure my child understands these.

Signed (parent/carer):

Date:

ACCEPTABLE USE OF THE ACADEMY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, ADVISORY BOARD, VOLUNTEERS AND VISITORS

Name of staff member/ advisory board /volunteer/visitor:

When using the academy's ICT systems and accessing the internet in the academy, or outside the academy on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the academy's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the academy's network
- Share my password with others or log in to the academy's network using someone else's details
- Take photographs of students without checking with the school home support first
- Share confidential information about the academy, its students or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the academy

I will only use the Academy's ICT systems and access the internet in the academy, or outside the academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the academy will monitor the websites I visit and my use of the Academy's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the academy, and keep all data securely stored in accordance with this policy and the academy's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the academy's ICT systems and internet responsibly, and ensure that students in my care do so too.

I understand and will undertake the responsibilities set out in the filtering and monitoring section (8.5) of the academy's Online Safety Policy.

Signed (staff member/ advisory board /volunteer/visitor):

Date:

ONLINE SAFETY TRAINING NEEDS AUDIT

Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in the academy?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the academy's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the academy's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the academy's ICT systems?	
Are you familiar with the academy's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: Online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

