



Device and Digital Conduct Policy

Last review date:		September 2026	
Next review date:		September 2027	
Responsible:		J. Hardwick	
Statutory Policy:		Yes	
Date	Version	Reason for change	Review
15/09/2026	1.0	New Policy	Annually

To be read alongside all relevant BOA Digital Technologies Academy policies and procedures including Behaviour Policy

Contents

1. Statement of intent.....	3
2. Our Approach	3
3. Legal Framework	4
4. Definitions	4
5. Roles and Responsibilities	5
6. Expectations of Mobile Devices within the Academy.....	7
7. Safeguarding	9
8. Acceptable Use.....	10
9. Confiscation of Devices	11
10. Monitoring and review	14

1. Statement of intent

At BOA Digital Technologies Academy, we are committed to creating a calm, focused and purposeful learning environment where all students can thrive. We recognise that clear and consistent expectations are essential in enabling high-quality teaching, strong relationships and positive behaviour across the academy. In line with the Department for Education's statutory guidance and the Children's Wellbeing and Schools Act 2026, the academy operates as a mobile phone-free environment throughout the school day. This supports a safe, disruption-free environment in which all students are Ready, Respectful and Safe. This policy extends to mobile phones and other personal smart technologies with similar communication or recording functionality.

Beyond maintaining high standards of behaviour, this policy plays a key role in supporting students' emotional wellbeing. We aim to create space for meaningful face-to-face interaction, enabling students to develop confidence, resilience and strong social skills. In an age where digital communication can replace real-world interaction, it is vital that students are supported to build positive relationships and navigate social situations effectively.

This approach also promotes a healthy and balanced relationship with technology. As a digital academy, we are committed to preparing students for the modern and also recognise that digital literacy extends far beyond mobile phone use. Through our curriculum, students develop the knowledge, skills and awareness to use technology purposefully, safely and responsibly. We ensure that technology is used as a tool for learning, creativity and innovation, rather than a distraction.

Ultimately, this policy strengthens our learning environment, supports positive wellbeing and social development, and ensures that students are equipped with the digital understanding and behaviours needed to succeed in modern society.

Staff will apply this policy consistently and use the clearly outlined approaches within the behaviour policy when addressing breaches.

2. Our Approach

Our approach is simple, consistent and captured in the phrase 'Responsible Digital Use'. As a digital academy, we recognise the importance of educating young people on the appropriate, responsible and purposeful use of technology. We are committed to ensuring that students develop a clear understanding of when, where and how digital technology should be used. Through our curriculum and wider academy experiences, students are taught to use technology as a tool for learning, creativity and appropriate communication, rather than passive consumption or distraction in a professional environment. During the school day, personal mobile and smart communication devices must remain inaccessible unless a specific, authorised exception applies for safeguarding or medical needs.

This policy is fully aligned with the academy's behaviour policy, Department For Education requirements and approach, which is centred on teaching behaviour, developing social skills and using restorative practice. Expectations around devices are taught explicitly, reinforced consistently and addressed through clear routines. Where expectations are not met, staff will respond in line with the behaviour policy, using a graduated approach that supports students to reflect, understand the impact of their choices and make better decisions moving forward.

By combining clear boundaries with education and support, our approach ensures that students not only meet expectations within the academy, but also develop the awareness, self-regulation and digital responsibility required beyond school.

3. Legal Framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Children's Wellbeing and Schools Act 2026
- DfE mobile phone guidance DfE (2026) 'Mobile phones in schools' (statutory guidance)
- DfE (2026) 'Keeping children safe in education 2026' DfE (2026) 'Keeping children safe in education 2026'
- The Education Act 2011
- The Education and Inspections Act 2006
- The Education Act 1996 (as amended)
- The Equality Act 2010
- The Children and Families Act 2014
- The Data Protection Act 2018 and UK GDPR
- DfE (2026) 'Suspension and permanent exclusion from maintained schools, academies and pupil referral units in England, including pupil movement'
- The Voyeurism (Offences) Act 2019
- DfE guidance on Searching, Screening and Confiscation (2022)

This policy operates in conjunction with the following academy policies:

- Complaints Procedures Policy
- Special Educational Needs and Disabilities (SEND) Policy
- Suspension and Exclusion Policy
- Child Protection and Safeguarding Policy
- Searching, Screening and Confiscation Policy
- Physical Restraint and Intervention Policy
- Anti-bullying Policy
- Relationships For Learning (Behaviour Policy)

4. Definitions

For the purpose of this policy, the following definitions apply:

Mobile Phone

A handheld electronic device designed primarily for communication, including making calls, sending messages, accessing the internet, using applications and capturing photos or videos. Mobile phone usage extends to both Smart and Non Smart devices.

Smartwatch / Wearable Device

A wearable electronic device that connects to a mobile phone or network and is capable of receiving notifications, messages, calls, or accessing applications and the internet.

Audio Device (Headphones/Earbuds)

Any wired or wireless device used to listen to audio from a mobile or digital device, including Bluetooth earbuds, headphones or similar equipment.

Recording Device

Any device capable of capturing images, video or audio, whether as a primary function or as part of a wider device (e.g. mobile phones, tablets or wearable technology).

Tablet Device

A portable touchscreen computer that enables internet access, application use, media consumption, communication and content creation.

Personal Laptop / Portable Computer

A personal, non-academy issued computing device capable of accessing the internet, running software applications and storing or transmitting data.

Handheld Gaming Device

A portable electronic device designed for gaming which may also include internet connectivity, communication features or media playback.

Internet-Enabled Device

Any device capable of connecting to the internet, including through Wi-Fi, mobile data or tethering, and accessing online platforms such as social media, messaging or web-based content.

The academy reserves the right to classify any similar or future technology as a mobile device where it meets the above criteria.

5. Roles and Responsibilities

The governing body is responsible for:

- Ensuring the policy reflects current DfE guidance and statutory expectations
- Supporting the academy in maintaining high standards of behaviour and safeguarding
- Monitoring the effectiveness of the policy

The Principal and Leadership Team (Senior and Extended)

- Ensuring the consistent implementation of this policy across the academy
- Establishing clear expectations and routines regarding mobile device use
- Supporting staff in the effective application of the policy
- Monitoring patterns of behaviour and responding to trends
- Communicating expectations to students, staff and parents
- Ensuring alignment with the Behaviour Policy, Safeguarding Policy and Searching & Confiscation procedures

All staff are responsible for:

- Modelling the same high standards expected of students by keeping personal mobile phones and smart devices out of sight and not using them for personal reasons in lessons, during active duties, while supervising students or in other pupil-facing areas

- Restricting personal use of mobile phones to appropriate staff-only spaces and non-supervisory break periods, except where an urgent personal matter has been agreed with a line manager
- Using personal devices only where necessary for an authorised professional purpose, such as multi-factor authentication, safeguarding or emergency communication, and doing so discreetly and proportionately
- Never using a personal device to take, store or share photographs, video or audio recordings of students. Academy-approved equipment and systems must be used for authorised recording or photography
- Following the Staff Code of Conduct, safeguarding expectations and data protection requirements at all times. Misuse by staff will be addressed through the appropriate staff conduct, safeguarding and/or disciplinary procedures

Teaching staff are responsible for:

- Consistently applying the expectations of this policy in lessons and around the academy
- Tutors ensure that all students have secured their personal devices in their lockable pouches as part of morning routine check
- Provide reminders of expectations to students when required
- Challenging and addressing mobile device use in line with academy routines
- Following agreed procedures for confiscation and recording incidents
- Using the academy behaviour systems to address breaches

Pastoral staff including Heads of Key Stage/Year are responsible for:

- Supporting the consistent application of the policy across the academy
- Monitoring repeated breaches and implementing targeted interventions
- Communicating with parents regarding concerns around mobile device use
- Implementing additional measures (e.g. phone hand-in systems) where required
- Supporting restorative conversations and behaviour reflection

Non-teaching staff are responsible for:

- Upholding and reinforcing expectations across all areas of the academy
- Challenging mobile device use where appropriate
- Reporting concerns or repeated issues to teaching or pastoral staff

Students are responsible for:

- Placing mobile devices in personal lockable pouches at the start of the day
- Ensuring devices are switched off prior to secure storage
- Handing over any devices immediately when requested by a member of staff

Parents/carers are responsible for:

- Supporting the academy's expectations and reinforcing them at home
- Not contacting students directly during school hours
- Communicating through the academy office where necessary
- Working in partnership with the academy to address any concerns

6. Expectations of Mobile Devices within the Academy

The academy operates a clear expectation that personal mobile phones, smartwatches and other personal communication devices are not accessible during the school day. BOA Digital is a technology-rich academy and actively promotes the purposeful use of digital technology for learning. Academy-issued or academy-approved tablets and laptops may therefore be used when directed by staff for a clear educational purpose and in accordance with the academy's acceptable-use, filtering and monitoring expectations. Personal tablets or laptops must remain closed, switched off or stored out of sight until a member of staff has explicitly authorised their use. Mobile phones are not included within any bring-your-own-device arrangement.

Responsibility for Personal Devices

Personal devices and accessories are brought onto academy premises, trips, visits and residential at the owner's risk. Students remain responsible for the security and condition of any personal device or accessory they choose to bring to the academy. The academy does not accept responsibility for loss, theft, accidental damage or deterioration of personal devices or accessories. Where an item is formally confiscated or placed into academy storage, reasonable steps will be taken to keep it secure.

Contact with home

During the school day, communication between parents/carers and students should be directed through main reception or another agreed academy route. Parents/carers should not contact students directly on a personal or academy device during the school day, and students should not use a personal device or academy device to contact home unless specifically authorised by a member of staff. Any unauthorised use or contact will be managed in accordance with this policy and the Behaviour Policy.

Mobile Phones

Mobile phones must be switched off and secured in the student's assigned lockable pouch for the duration of the school day. They must not be accessed or used in lessons, during transitions, at social times or elsewhere on the academy site unless an authorised exception applies.

Phone Pouches

Academy-issued phone pouches form part of the academy's arrangements for maintaining a mobile phone-free environment. Students must take reasonable care of their assigned pouch and must not deliberately damage, cut, force open, tamper with, disable or otherwise interfere with it. Deliberate damage or tampering with a pouch, including

attempts to circumvent the academy's mobile phone arrangements, will be addressed in accordance with the Academy Behaviour Policy.

Smartwatches / Wearable Devices

Smartwatches and devices are considered within the same context as mobile phones and follow the same expectations around acceptable use.

Handheld Gaming Devices

Handheld gaming devices are not permitted for use in the academy. Such devices must be switched off and stored securely; any unauthorised use will result in confiscation.

Other Internet-Enabled Devices

Personal devices capable of internet access, messaging or social media access must not be used during the academy day unless they fall within an authorised learning, medical, safeguarding or reasonable-adjustment exception. Personal hotspots, tethering, virtual private networks (VPNs), proxy services or any other technology or method intended to bypass the academy's filtering, monitoring or network security must not be used. Any attempt to circumvent academy filtering, monitoring or network restrictions will be treated as serious misbehaviour and addressed in accordance with the Academy Behaviour Policy.

Use of Headphones and Audio Devices

Headphones, earbuds and all personal audio devices are not permitted to be used during the school day. Students must ensure that any headphones or audio devices are switched off, stored out of sight (e.g. in bags) and not worn around the academy at any time.

Media and Recording Devices

Personal devices must not be used to take photographs, record video or audio, or share recordings of any student, member of staff or visitor without explicit academy authorisation. Recording using a personal device is prohibited across the academy site and is particularly serious in toilets, changing areas and other private or sensitive spaces.

Any misuse will be assessed for safeguarding implications and, where appropriate, treated as serious misbehaviour under the Academy Behaviour Policy. Content that harms others, breaches privacy or has the potential to bring the academy or its community into disrepute may result in further sanctions and/or referral to the DSL or external agencies.

Staff Use of Personal Mobile Devices

Staff personal mobile phones must remain out of sight and must not be used for personal reasons during lessons, active duties, direct supervision of students or in pupil-facing areas. Where a device is required for an authorised professional purpose, safeguarding matter, emergency communication or multi-factor authentication, its use should be brief, discreet and proportionate. Staff must not use personal devices to photograph, film or record students; academy-approved devices and systems must be used for any authorised image, video or audio capture.

Trips, Visits and Residentials

The expectations of this policy extend to academy trips, visits and residentials, including activity outside the normal school day. The trip leader will communicate the specific device arrangements in advance. Where students are permitted to bring a personal device, it must remain switched off or otherwise secured and out of sight unless the trip leader explicitly authorises access for a safeguarding or essential communication purpose, for example to contact the designated trip phone.

Students must not use personal devices on trips or residentials to take or share photographs, video or audio recordings of students, staff or others. Content must not be posted, shared or used in a way that compromises safeguarding, privacy, the welfare of others or has the potential to bring the academy into disrepute. The trip leader may require devices to be stored centrally for specified periods, including overnight, where this supports safeguarding or the safe running of the visit.

Students must be able to raise safeguarding concerns with staff, including concerns about online activity. Where access to a device is necessary to explain or evidence such a concern, this will be facilitated safely by staff. Misuse by a student during a trip or residential will be managed in accordance with the Academy Behaviour Policy and may include confiscation or restriction of access for the remainder of the activity, subject to safeguarding and individual circumstances.

Staff on trips and residentials remain subject to the staff expectations in this policy. Personal devices should not be used for personal reasons while actively supervising students and must not be used to capture images or recordings of students. Academy-approved equipment, designated trip phones and approved communication channels should be used for safeguarding, emergency and operational purposes wherever practicable.

7. Safeguarding

Safeguarding is of the utmost importance at BOA Digital Technologies Academy and underpins all aspects of academy life. This policy is designed to support the safety, wellbeing and protection of all students and staff by reducing risks associated with the misuse of mobile devices.

An extensive range of evidence demonstrates that mobile devices present a number of safeguarding risks, including but not limited to: the unauthorised recording or sharing of images and videos, cyberbullying, exposure to inappropriate or harmful content, and communication with individuals outside of the academy in an unsafe or unregulated manner. By prohibiting the use of mobile devices during the school day, the academy significantly reduces these risks and ensures that all students can learn and socialise in a safe and secure environment.

This policy aligns with the statutory guidance set out in Keeping Children Safe in Education (KCSIE) 2026 and the Children's Wellbeing and Schools Act 2026. The academy

recognises its duties to safeguard and promote the welfare of children, including protecting students from child-on-child abuse, online harm, exploitation and inappropriate use of technology. Behaviours such as photographing or recording others without permission, sharing harmful or inappropriate content, or engaging in unsafe online communication may constitute safeguarding concerns and will be treated with the seriousness they require.

Safeguarding concerns arising from digital technology may include the creation, requesting, sending or sharing of nudes and semi-nudes, including AI-generated, digitally manipulated or synthetic sexual imagery; deepfakes or other manipulated images, audio or video; cyberbullying; impersonation; harmful online communication; and the recording or sharing of others without permission.

Any such incident will be considered for safeguarding implications and referred to the Designated Safeguarding Lead (DSL) where appropriate. Safeguarding concerns will be managed in accordance with the Academy Child Protection and Safeguarding Policy. Where the incident involves student conduct or a breach of academy expectations, it will also be addressed in accordance with the Academy Behaviour Policy. External agencies, including the police or children's social care, may be involved where appropriate.

All staff have a responsibility to remain vigilant and act promptly where safeguarding concerns arise. Students are also educated through the curriculum and wider academy life about safe, responsible and respectful use of technology, ensuring they understand both the risks and their responsibilities.

By maintaining clear boundaries around mobile device use, this policy plays a critical role in protecting all members of the academy community and ensuring that safeguarding remains at the centre of our practice.

8. Acceptable Use

Whilst mobile phones are not permitted for general use during the school day, BOA Digital Technologies Academy recognises the importance of educating students on the appropriate, safe and responsible use of technology. Acceptable use is therefore clearly defined and applies where the use of a device is explicitly permitted by the academy and for the purpose of learning.

Where artificial intelligence (AI) tools are permitted for educational use, students must use them only for the purpose authorised by a member of staff and in accordance with academy expectations. AI must not be used to impersonate another person; bully, harass, humiliate or intimidate others; create deceptive or harmful content; manipulate images, audio or video of another person; or create inappropriate or sexualised content.

Where use is permitted, students must

- Use devices responsibly and in line with academy expectations

- Only use or access when explicitly authorised by a member of staff for a clear educational purpose or essential communication
- Not impact the safety, wellbeing or learning of others
- Follow all instructions given by the member of staff
- Ensure all content accessed is appropriate and lawful
- Keep passwords, PINs, authentication codes and account credentials private; students must not access another person's account, allow another person to use their account, or attempt to obtain another user's login information
- Respect the privacy and dignity of others
- Not bring the Academy into disrepute

The following behaviours are **not acceptable under any circumstances**:

- Taking photos or videos on a personal device, or using any device to record an individual without explicit academy authorisation
- Recording audio without permission
- Sharing images, videos, audio or content relating to the academy or its community without authorisation, particularly where this could compromise safeguarding, privacy or bring the academy into disrepute
- Accessing or displaying inappropriate or harmful content
- Using VPNs, proxy services, personal hotspots, tethering or other methods to bypass the academy's filtering, monitoring or network security
- Using AI or other digital tools to impersonate another person; create, alter or share deceptive or harmful images, audio or video, including deepfakes; or to bully, harass, humiliate or intimidate others
- Creating, requesting, sending or sharing nudes and semi-nudes, including AI-generated, digitally manipulated or synthetic sexual imagery of another person
- Using devices to communicate in a way that could cause harm, distress or disruption
- Using devices in toilets, changing areas or other private spaces

Any use of a mobile device that breaches these expectations will be treated as a violation of the academy's behaviour and safeguarding standards and will be addressed in line with the Behaviour Policy.

This approach ensures that students develop a clear understanding of appropriate digital conduct, recognising that access to technology is a privilege that comes with responsibility. Through this, students are supported to build the awareness, judgement and self-regulation required to use technology safely and appropriately both within and beyond the academy.

9. Confiscation of Devices

BOA Digital Technologies Academy will enforce this policy consistently to maintain a calm, safe and disruption-free environment. In line with DfE guidance on Searching, Screening and Confiscation and the academy's own Searching and Confiscation Policy, staff may confiscate a device being used or accessed in breach of academy rules. Any

confiscation will be reasonable, proportionate and mindful of relevant individual circumstances.

Where a device is seen, heard or used in breach of this policy, it will be confiscated by a member of staff.

Procedure for Confiscation

- The student will be instructed to hand over the device immediately
- The device will be switched off (if not already) and retained securely
- The confiscation will be logged in line with academy behaviour systems
- The device will be returned to the student at the end of the school day
- Should a student refuse to hand over a device when instructed, the matter will be escalated in line with the Academy Behaviour Policy as a refusal to follow a reasonable instruction and a serious breach involving an item prohibited by academy rules in those circumstances.

Where appropriate, the academy may require devices to be collected by a parent/carer, particularly in cases of repeated breaches or where the misuse of a device raises safeguarding concerns. In such instances, the matter will be risk assessed internally and managed in line with the academy's safeguarding procedures and Keeping Children Safe in Education (KCSIE) 2026. Where necessary, this may include referral to external agencies, including the Local Authority or the police.

Refusal to hand in a mobile device on request

If a student refuses to hand over a mobile device:

- This will be treated as a refusal to follow a reasonable instruction and as serious misbehaviour involving an item prohibited by academy rules in those circumstances
- The incident will be escalated in line with the Behaviour Policy
- This may result in sanctions including detention, internal reflection or suspension
- Parents/carers will be informed

Searching for Devices

In line with DfE guidance, authorised staff may search a student or their possessions where there are reasonable grounds to suspect that the student is in possession of a prohibited item or an item that has been used in breach of academy rules.

- Searches will be conducted respectfully and in line with the academy's Searching and Screening Policy
- Wherever possible, searches will be conducted with the student's consent and with a second member of staff present
- If a device is found, it will be confiscated in accordance with this policy

Content on Devices

Staff will not routinely search the digital content of a device. However, in exceptional circumstances where there is a safeguarding concern:

- A senior member of staff may examine the device where it is lawful and appropriate to do so
- Any content that raises safeguarding concerns may be referred to the Designated Safeguarding Lead (DSL)
- Where necessary, devices may be passed to external agencies, including the police

Repeated Breaches

The academy will use a clear graduated response to repeated breaches. The response may be adapted where safeguarding or medical needs.

First breach

The student will be directed to Internal Reflection following a serious breach of the Academy's Mobile Device Policy and in accordance with the Academy Behaviour Policy. The device will be confiscated, the breach recorded, and the device will normally be returned at the end of the school day in accordance with the confiscation procedure.

Repeated breach

A repeated breach may result in suspension, where this is lawful, reasonable and proportionate, in accordance with the Academy Behaviour Policy. The device will be confiscated, parental collection required and a time-limited central storage arrangement will be introduced for a defined review period. The student will hand the device to a designated academy storage point on arrival each day and collect it at the end of the school day. A parental meeting will be held to review the repeated breach, reinforce expectations and agree any additional support required.

Further subsequent breaches

Further breaches will result in escalation in line with the Academy Behaviour Policy. The academy may also consider whether an off-site direction is appropriate as a temporary intervention intended to improve future behaviour.

Where a breach involves recording, sharing content, online abuse, intimidation, the creation, requesting, sending or sharing of nudes and semi-nudes (including AI-generated, digitally manipulated or synthetic sexual imagery), deepfakes, harassment, privacy concerns or another safeguarding risk, it will be considered for safeguarding implications, referred to the DSL where appropriate, and addressed in accordance with the Academy Child Protection and Safeguarding Policy and Academy Behaviour Policy. External agencies may be involved where required.

10. Monitoring and review

This policy will be reviewed by the Principal and Governing Body on an annual basis; they will make any necessary changes and communicate these to all members of staff and relevant stakeholders.