LDBS Academies Trust
LAT and LAT 2

ADOPTION GUIDANCE AND POLICY CHANGE LOG
Mobile Phones and Smart Technology Policy

PLEASE REMOVE THIS PAGE UPON ADOPTION BY THE LOCAL GOVERNING BODY AND BEFORE PUBLICATION ON THE WEBSITE / SHARED DRIVE AND COMMUNICATION TO STAFF / OTHER RELEVANT PARTIES. AFTER DOING SO, PLEASE UPDATE THE TABLE OF CONTENTS!

General guidance for Headteachers and Local Governing Bodies (LGBs):

- This Policy sets minimum compliance requirements for all LATMAT (LAT and LAT 2) schools.
- A space has been foreseen in the header of this Policy, for the school can add its own name and logo.
- A box has been foreseen below the Trust vision, for the school to add its school-specific vision.
- Annex 1 must be completed by the school with the school-specific information before it is submitted to the LGB for adoption.
- It is the responsibility of the LGB to:
    - Approve this Policy (with Annex 1 - School-specific details completed);
    - Ensure local implementation complies with this template.

Any concerns regarding the Policy should be raised with the Trust via the local Governance Professional. Please do not change the formatting of titles etc as the document contains cross-references.

Generic changes to all policy documents in 2026 -27:

- Change of the registered address of both LDBS Academies Trust and LDBS Academies Trust 2. The registered address is now: Park Lane, London, England N17 0HH
- New Articles of Association, approved by the DfE in Aug 2026 (to be ratified by Members) changes the name of the Local Academy Committees (and LAC members) to Local Governing Bodies (and local governors). The terminology in this policy has been updated to reflect the new Articles.
- Name of new Chair of the Board of Directors, Peter King

Changes to this policy document since its last revision (as a result of KCSIE Sept 2026 updates):

- AI, deepfake and AI-generated imagery safeguarding provisions.
- The four online safety risk categories: content, contact, conduct and commerce.
- Harmful online influence, misogyny, misandry, extremist content and misinformation.
- Clear reporting and handling expectations for harmful or illegal imagery.
- Filtering and monitoring responsibilities and annual governance oversight.
- Visitors' personal device storage and proportionate exceptions for governors, directors and visiting professionals.
- An unambiguous default position that pupils must not bring personal devices onto the school site unless explicitly authorised and recorded.

- Smart watches with communication, recording, camera, internet or AI functionality treated in the same way as mobile phones.
- Human review required before AI-generated content is used for safeguarding decisions, fact verification or wellbeing assessments.
- Clear conditions for staff personal device use during breaks, PPA and off-duty periods.
- Contractors and agency personnel required to comply as a condition of site access.

[Add school logo and name]

part of the

LDBS Academies Trust

LAT and LAT 2

Mobile and Smart Technology Policy

Document type	Trust Policy	Statutory DfE / Trust	Trust
Approval Level	Trust Board of Directors	Review Frequency	Annual
Approval date	01/10/2026	Next Review Date	30/09/2027
On behalf of the Trust Board of Directors			
Name	Peter King	Name	Christalla Jamil
Position	Chair of the Board of Directors	Position	CEO
On behalf of Choose an item.			
Name		Name	
Position	Chair of the School Governing Body	Position	Headteacher
Publication to	☒ GovHub	☒ Staff info site	☒ Website

Trust Vision Statement

"The kingdom of heaven is like a mustard seed, which a man took and planted in his field. Though it is the smallest of all seeds, yet when it grows, it is the largest of garden plants and becomes a tree, so that the birds come and perch in its branches." (Matthew 13: 31-32)

In the parable of The Mustard Seed, Jesus reminds us that even the smallest of seeds has the potential to grow into the fullness of itself. We aim to provide the right environment for our children, and all whom we serve, to flourish into the fullness of themselves. He tells us these seeds grow into trees, capable of providing a home for a rich diversity of life, our work is to ensure all in our communities grow into people of compassion and wisdom with a deep spiritual understanding of how to support the needs of others.

SCHOOL VISION

Click or tap here to enter text.

Table of Contents

Mobile and Smart Technology Policy 3

1 Aims 5

2 Legislation and Statutory Guidance 5

3 Definitions 5

4 Acronyms 6

5 Roles and Responsibilities 6

5.1 The Headteacher 6

5.2 Staff 6

5.3 Pupils 7

5.4 Parents / carers 7

6 Safe use of mobile and smart technology 8

7 School-provided mobile phones and devices (e.g. laptops, tablets) 8

8 Searching, screening and confiscation of electronic devices 8

9 Visitors' use of mobile and smart technology 9

10 Responding to policy breaches 9

11 Links with other policies 10

12 Policy monitoring and review 10

ANNEX I – SCHOOL-SPECIFIC INFORMATION RELATED TO THIS POLICY 11

1 Aims

The purpose of this Policy is to safeguard and promote the welfare of all members of our schools' communities when using mobile devices and smart technology.

The LDBS Academies Trust (LAT and LAT 2) and its family of schools recognise that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm when using mobile and smart technology.

As outlined in the Trust's Child Protection Policy, the school's Designated Safeguarding Lead (DSL) (see Annex I) has overall responsibility for online safety.

This policy applies to all access to and use of all mobile and smart technology on site; which includes but is not limited to mobile/smart phones and personal devices such as tablets, ereaders, games consoles and wearable technology, such as smart watches and fitness trackers, which facilitate communication or have the capability to record sound and/or images.

The Trust's default position is that pupils must not bring personal mobile phones or smart devices onto the school site. Any exception must be explicitly authorised by the Headteacher and recorded.

This policy applies to pupils, parents/carers and all staff, including members of the Local Governing Body (LGB), the leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy).

2 Legislation and Statutory Guidance

This policy is based on statutory guidance from the Department for Education (DfE): 'Keeping Children Safe in Education 2026' (KCSIE), Early Years and Foundation Stage (EYFS), 'Working Together to Safeguard Children' (WTSC), the DfE non-statutory guidance 'Behaviour in Schools', 'Searching, screening and confiscation in schools', 'Mobile Phones in Schools'.

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

3 Definitions

Staff	All individuals who work for, or provide services on behalf of the setting, including the leadership team, teachers, support staff, kitchen staff, members of the Local Governing Body (LGB), Trust central team members, external contractors, visitors, volunteers and any other individuals who work for or provide services on behalf of the setting.
Smart watch	A smart watch with messaging, internet, camera, recording, AI or other communication functionality is treated in the same way as a mobile phone for the purposes of this Policy.
Visitor	Any person attending the school who is not a pupil or member of staff, including parents and carers, local governors, Trust directors, contractors and visiting professionals.

4 Acronyms

AI	Artificial Intelligence
AUP	Acceptable Use Policy
DDSL	Deputy Designated Safeguarding Lead
DSL	Designated Safeguarding Lead
LGB	Local Governing Body
LADO	Local Authority Designated Officer
SLT	Senior Leadership Team

5 Roles and Responsibilities

5.1 The Headteacher

The headteacher is responsible for monitoring the implementation of this policy, and holding staff and pupils accountable for its implementation and communicating the requirements and consequences of non-compliance.

The Headteacher must ensure that the school has:

- Lockable storage where devices can be stored during the school day
- clear emergency circumstances in which staff may use a personal device during teaching periods;
- defined and recorded exceptions permitting pupils to bring a personal device onto the school site, limited to genuine safety or medical needs;
- a procedure for authorised pupil devices to be switched off, handed in, stored securely and collected at the end of the day;
- risk assessments and recorded, time-limited permissions where personal devices are exceptionally required for school business;
- visitor arrangements that identify where devices will be stored and how proportionate exceptions will be authorised;
- school devices for activities involving pupil images, direct work with pupils, remote learning or communications with parents and carers;
- appropriate signage, induction and AUP arrangements for visitors and volunteers;
- filtering and monitoring arrangements that address risks arising from mobile and smart technology, including generative AI.

5.2 Staff

All staff, including supply and agency staff, are responsible for consistently implementing this Policy.

Staff must:

- keep personal mobile and smart devices secure, switched off or on silent/do not disturb during teaching periods;

- disable or hide Bluetooth, AirDrop and similar communication functions during teaching periods;
- not use a personal device during teaching periods unless written permission has been given by SLT for an exceptional reason;
- not use a personal device to contact pupils or parents and carers;
- use school-provided equipment to take pupil photographs or videos, work directly with pupils, deliver remote learning, or communicate with parents and carers, unless a documented exception has been approved following risk assessment;
- report suspected breaches involving visitors to the DSL.

Staff may use personal phones or smart devices during lunch breaks, PPA time and other off-duty periods only in designated staff-only areas, such as staff rooms or offices, and only where pupils are not present. Such use must remain professional, must not interfere with duties, supervision or safeguarding responsibilities, and must comply with the restrictions in this Policy, the Staff Professionalism and Code of Conduct and the AUP.

If a member of staff breaches this Policy, action will be taken under the Child Protection Policy, Staff Professionalism and Code of Conduct and Disciplinary Procedure. Suspected illegal content or criminal use will be referred to the police and, where appropriate, the LADO..

5.3 Pupils

Pupils must not bring personal mobile phones or smart devices onto the school site unless specifically authorised by the Headteacher. Any authorisation must be explicit, recorded and communicated to the pupil's parents or carers, together with the applicable conditions.

Exceptions will be limited to extenuating circumstances, such as a safety need connected with travel to and from school or an agreed medical need. Unless an authorised medical arrangement states otherwise, an approved device must be switched off and handed in at the start of the day for secure storage under the school's procedure. It may be collected at the end of the day.

The searching and confiscation provisions in section 8 apply if a pupil brings a device onto the site without authorisation, fails to hand in an authorised device, or misuses a device. Their inclusion does not create permission for pupils to bring devices onto the site.

Pupils who need to contact a parent or carer during the school day must use the school office arrangements. Personal devices must not be taken into examinations. Home use for learning must comply with the AUP.

Pupils will receive age-appropriate education about safe and appropriate use, the four online safety risk categories of content, contact, conduct and commerce, and harmful online influence, discriminatory content, misogyny, misandry, extremism, misinformation and disinformation..

5.4 Parents / carers

Parents and carers should contact the school office if an urgent message must be passed to their child. Requests for an exceptional pupil device arrangement, including for medical monitoring, must be agreed with the Headteacher in advance and documented in writing..

6 Safe use of mobile and smart technology

The Trust and its schools recognise that use of mobile and smart technologies is part of everyday life for many pupils, staff and parents/carers.

Mobile and smart technology may expose users to risks relating to content, contact, conduct and commerce. The school will use its safeguarding procedures and curriculum to help pupils recognise, avoid and report these risks.

The Trust recognises that generative artificial intelligence (AI) tools may present safeguarding risks, including exposure to harmful content, simulated harmful interactions, grooming, bullying, harassment, and the creation or sharing of manipulated images, audio or video, including deepfakes and AI-generated nude or semi-nude images. Pupils must not use AI tools to create, request, share or distribute content that may harm another person. Concerns involving AI-generated content will be managed in accordance with the Child Protection and Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy and AI Policy.

Any pupil reporting online abuse, cyberbullying, exploitation, grooming, harassment or another concern relating to mobile or smart technology will be listened to, taken seriously, reassured that they have done the right thing by reporting it, and supported in accordance with the Child Protection and Safeguarding Policy.

Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of our community are advised to:

- take steps to protect their personal mobile phones or other smart devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on personal phones or devices.
- Mobile devices and other forms of smart technology are not permitted to be used in specific areas on site and when visiting other sites; this includes toilets, changing rooms and swimming pools.
- The sending of abusive or inappropriate messages or content, including via personal mobile devices and/or smart technology is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and child protection policies.
- All members of the Trust community are advised to ensure that their personal mobile and smart technology devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.

7 School-provided mobile phones and devices (e.g. laptops, tablets)

School-provided laptops, tablets, phones and other devices must be password or PIN protected and used in accordance with relevant Trust and school policies. Users will be informed through the AUP that activity may be monitored for safeguarding and compliance purposes.

8 Searching, screening and confiscation of electronic devices

- Pupils must not bring personal mobile phones or smart devices onto the school site unless specifically authorised by the Headteacher. This section applies if a device is brought onto the site without authorisation, is not handed in as required, or is misused.

- Staff may confiscate a pupil's device where they reasonably believe it has been brought onto the site or used in breach of this Policy or another Trust policy.
- A confiscated device will be stored securely and normally released to a parent or carer in accordance with the school's procedure.
- Where potentially indecent or AI-generated nude or semi-nude imagery is suspected, staff must confiscate the device without viewing the content and refer the matter urgently to the DSL or DDSL.
- Staff must not view, copy, print, share, store, save or delete such imagery, ask a pupil to share, download or delete it, or investigate the incident themselves. Accidental viewing must be reported to the DSL immediately.
- Suspected illegal data or evidence of a criminal offence must be preserved and the device passed to the police as soon as reasonably practicable.
- Any search or examination of a device must follow the Behaviour Policy, Child Protection and Safeguarding Policy and Department for Education guidance on searching, screening and confiscation.
- The DSL must be informed promptly where a search indicates a safeguarding risk or concerns a prohibited item.
- Data must not be erased if it may be evidence of an offence. Any decision to examine or erase data must be made only by an authorised person and must meet the applicable legal and policy test.

9 Visitors' use of mobile and smart technology

- Visitors should normally keep personal mobile phones and smart devices switched off or on silent and securely stored. Each school must identify its local storage arrangement, such as a secure locker, locked school-office storage or retention in the visitor's locked vehicle, and communicate this at sign-in.
- Local governors and Trust directors are covered by this section. They may retain a device where this is necessary for their role and has been authorised, provided that it remains on silent and is not used in pupil areas except in an emergency.
- Visiting professionals, including social workers, educational psychologists, NHS staff and emergency-service personnel, may retain and use a work device where the Headteacher or an authorised member of staff is satisfied that this is necessary for their professional role. The decision must be proportionate to the visit, informed by risk assessment where appropriate, and recorded. Any photography, recording or processing of pupil information must comply with the visitor's professional duties, data protection requirements and school instructions.
- Contractors and agency personnel must comply with this Policy as a condition of accessing school premises.
- All visitors must follow school signage and instructions, comply with the Visitor and Volunteer AUP where applicable, and expect to be challenged if staff have a safeguarding concern about device use. Suspected breaches must be reported to the DSL.

10 Responding to policy breaches

Policy breaches and concerns must be reported under the school's established safeguarding, behaviour, whistleblowing and online safety procedures. Pupil sanctions and support will follow the Behaviour Policy and Child Protection and Safeguarding Policy. Following an incident, leaders will identify lessons learned and make any necessary policy, procedure or curriculum changes.

11 Links with other policies

- Anti-bullying policy
- Acceptable Use Policies (AUP)
- Behaviour policy
- Child protection policy (including Online Safety)
- Complaints Procedure
- Data Protection Policy
- Relationships and Sex Education (RSE) and Health Education Policy
- Staff professionalism and code of conduct
- Whistleblowing Policy

12 Policy monitoring and review

The Trust will review this Policy at least annually and following relevant national or local updates, significant concerns, or changes to technical infrastructure.

The Trust and its schools will monitor internet and technology use through Trust and school-provided devices and systems and will evaluate whether filtering and monitoring controls remain effective.

The school and Local Governing Body will review mobile and smart technology risks, filtering and monitoring arrangements and relevant safeguarding incidents through the annual safeguarding review.

The annual review must consider trends, incidents, emerging technologies and the effectiveness of filtering and monitoring controls, with actions formally recorded in governance minutes.

[Insert school name and logo]

Annex I – School-specific Information related to this policy

Responsibilities	**Position**	**Name**
School Designated Safeguarding Lead	[position]	[name]
School Deputy Designated Safeguarding Lead	[position]	[name]

Local Authority LADO: [Provide details]

Location of the school's policies and procedures:

- Acceptable Use Policy: [location]
- Child Protection Policy: [location]
- Complaints Policy: [location]
- Online Safety Policy: [location]
- Whistleblowing policy: [location]