MOBILE & SMART TECHNOLOGY POLICY

Using technology safely. Protecting privacy.
Maintaining professional boundaries.



RIVERSIDE BRIDGE SCHOOL

INSPIRE, EMPOWER, ACHIEVE

This policy forms part of the Riverside Bridge School Policy Framework
and should be read alongside any related policies, procedures and guidance.

RIVERSIDE BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE

OUR COMMITMENT

At Riverside Bridge School, every policy reflects our commitment to creating a safe, inclusive and ambitious school community in which every pupil is valued, every voice matters and every family is respected and supported.

Our policies translate our values into consistent practice. They support high expectations, clear responsibilities, effective partnership and informed decision-making, ensuring that the needs, rights, wellbeing and future outcomes of our pupils remain at the heart of our work.

We work collaboratively, act with integrity and continually reflect upon and improve our practice to achieve the best possible outcomes for every pupil.

POLICY PRINCIPLES

Our Policy Principles underpin how we work together and guide the decisions and actions we take to support every pupil and their families.



POLICY PURPOSE & FRAMEWORK

Riverside Bridge School policies set out the expectations, responsibilities and approaches that support safe, consistent and high-quality practice across the school. They translate our values, statutory responsibilities and professional expectations into clear guidance for everyday decision-making and practice.

Each policy forms part of the Riverside Bridge School Policy Framework and should be read alongside any related policies, procedures, statutory guidance and school frameworks referenced within the document.

Policies apply to the members of the school community identified within each document, including staff, governors, parents and carers, volunteers, contractors and other professionals where relevant. Everyone is expected to understand and apply the requirements appropriate to their role and to seek further guidance where clarification is required.

CURRICULUM DRIVERS



Our Drivers provide a shared golden thread across curriculum, school life, policy and leadership, helping ensure that our decisions and practice remain focused on the experiences and futures we want for every pupil.

STATEMENT OF INTENT

This policy sets out Riverside Bridge School's approach to the safe, appropriate and responsible use of mobile phones, smart watches, wearable technology and other connected devices. It establishes clear expectations for pupils, staff, families, visitors and professionals so that technology does not compromise safeguarding, privacy, professional boundaries, effective supervision or the learning environment

At Riverside Bridge School, many pupils have complex communication, sensory, physical, medical and learning needs and may require high levels of adult support and supervision. Technology can provide important opportunities for communication, accessibility, learning, independence and safety. However, devices capable of recording, communicating, accessing the internet, tracking location or storing and sharing information also create significant safeguarding, privacy and data protection risks within a specialist school environment.

The school therefore operates a mobile-phone-free environment for pupils throughout the school day, while recognising that individual pupils may require access to particular technology because of disability, medical need, communication, safeguarding, independent travel or another identified need. Any exception will be considered individually, appropriately risk assessed and subject to proportionate safeguards.

Staff have a particular professional responsibility to ensure that personal technology does not interfere with pupil supervision or create inappropriate professional boundaries. Personal devices must not be used to photograph or record pupils, communicate privately with pupils or families, store school information or undertake other school activity except where specifically authorised within this policy.

Parents, carers, visitors, contractors and external professionals are also expected to use technology in a manner that protects the privacy, dignity and safety of pupils and staff while on the school site or participating in school activities.

Where concerns arise regarding a device or its use, the school will respond proportionately and in accordance with its safeguarding, data protection and other relevant procedures. Searching, confiscation or examination of a pupil's device will only take place where there is a lawful and justified basis for doing so.

The school will keep its approach under review as technology develops. New and emerging technologies, including artificial intelligence, wearable devices, location-tracking technology and remotely operated devices, will be considered according to their purpose, potential benefit and associated safeguarding, privacy and security risks.

Our responsibilities to pupils, staff and families

Riverside Bridge School will:

- maintain clear expectations for mobile and smart technology across the school;
- protect pupils' privacy, dignity and personal information;
- ensure personal technology does not compromise effective supervision or professional boundaries;
- provide appropriate arrangements for the secure storage of pupil devices;
- consider reasonable adjustments and individual exceptions where these are required;
- ensure school-approved technology is used safely and appropriately;
- respond promptly to safeguarding, privacy, security or data protection concerns;
- apply searching, confiscation and examination powers lawfully and proportionately;
- provide staff with appropriate guidance and training;
- ensure families and visitors understand the expectations that apply on the school site; and
- review arrangements as technology, legislation and safeguarding risks develop.

Through these arrangements, Riverside Bridge School aims to enable the benefits of technology while maintaining a safe, respectful and professionally accountable environment for every pupil.

TABLE OF CONTENTS

01	INTRODUCTION	02	SCOPE
03	ROLES AND RESPONSIBILITIES	04	STAFF USE OF MOBILE AND SMART TECHNOLOGY
05	USE OF MOBILE AND SMART TECHNOLOGY DURING OFF-SITE ACTIVITIES	06	USE OF MOBILE AND SMART TECHNOLOGY BY PUPILS
07	USE OF MOBILE AND SMART TECHNOLOGY BY PARENTS, CARERS, VISITORS AND EXTERNAL PROFESSIONALS	08	SEARCHING, SCREENING, CONFISCATION AND EXAMINATION OF DEVICES
09	ARTIFICIAL INTELLIGENCE (AI) AND EMERGING TECHNOLOGIES	10	LOSS, THEFT, DATA BREACHES AND INCIDENT REPORTING
11	MONITORING, COMPLIANCE AND REVIEW	12	RELATED POLICIES AND FRAMEWORKS

APPROVED BY: Governing Board

APPROVED ON: September 2026

REVIEWED DUE ON: September 2027

Section 01

INTRODUCTION

Setting expectations. Balancing opportunity and risk.

Riverside Bridge School is a specialist provision for pupils with a wide range of complex learning, communication, sensory, physical and medical needs. Safeguarding, dignity and the protection of personal information underpin every aspect of our practice. Mobile phones, smart watches and other connected technologies are an integral part of modern life and can support communication, learning and safety. However, they also present significant safeguarding, privacy, data protection and security risks if not managed appropriately within a specialist school environment.

In accordance with Department for Education guidance on mobile phones in schools, Riverside Bridge School operates as a mobile-phone-free environment throughout the school day. Pupils must not have access to mobile phones or smart technology with equivalent communication, internet or recording functionality during lessons, transitions, breaktimes, lunchtime or other school-supervised activities unless an individual exception or reasonable adjustment has been formally agreed by the school.

This policy establishes clear expectations for the safe, secure and appropriate use of mobile phones, wearable technology and other smart devices by staff, pupils, parents, carers, governors, visitors, contractors and external professionals. It supports the school's commitment to safeguarding children, maintaining professional boundaries, protecting confidential information and ensuring that technology does not interfere with learning, therapeutic provision or the safe operation of the school.

This policy should be read alongside the school's Online Safety Policy, Artificial Intelligence (AI) Guidance, Safeguarding and Child Protection Policy, Positive Support Policy, Data Protection Policy, Image Use Policy and Staff Code of Conduct.

The policy has been developed with regard to relevant legislation and Department for Education guidance, including, including:

- Keeping Children Safe in Education (KCSIE);
- Behaviour in Schools;
- Searching, Screening and Confiscation;
- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Equality Act 2010.

The aims of this policy are to:

- safeguard the privacy, dignity and well-being of pupils, staff and visitors;
- maintain a mobile-phone-free learning environment for pupils throughout the school day;
- promote safe, responsible and professional use of mobile and smart technology;

- protect confidential and personal information from unauthorised recording, sharing or storage;
- provide clear expectations for the use, storage, searching and confiscation of devices where necessary;
- ensure that all use of mobile and smart technology supports effective safeguarding practice across the school.

Section 02

SCOPE

Protecting pupils. Responding promptly. Reducing risk.

This policy applies to all members of the Riverside Bridge School community and to any individual using or bringing mobile or smart technology onto school premises or whilst participating in school-led activities. It sets out the expectations for the safe, appropriate and responsible use of personal and school-issued devices in order to safeguard pupils, protect confidential information and maintain a safe learning environment.

The policy applies to:

- all employees, including teachers, support staff, therapists, administrative staff, site staff and leadership;
- agency staff, volunteers, students and contractors;
- governors and trustees;
- pupils;
- parents and carers;
- visitors and external professionals.

For the purposes of this policy, mobile and smart technology includes, but is not limited to:

- mobile phones and smartphones;
- smart watches and wearable devices;
- tablets and laptops;
- e-readers and personal multimedia devices;
- Bluetooth or GPS-enabled tracking devices (including AirTags or similar products);
- devices capable of taking photographs, recording audio or video, accessing the internet, messaging, location tracking or using artificial intelligence applications.

This policy applies:

- throughout all school buildings and grounds;
- during educational visits, residential visits, community access activities, work-related learning and transport arranged or supervised by the school;
- during before and after-school activities organised by the school;
- whenever an individual is representing Riverside Bridge School or undertaking duties on behalf of the school.

The policy applies equally to personal and school-issued devices. Where separate procedures exist for the use of school-owned equipment, including approved educational technology, staff must also comply with those procedures.

Nothing within this policy overrides the school's statutory safeguarding responsibilities or duties under the Equality Act 2010. Where a pupil or member of staff requires the use of a mobile or smart device because of a disability, medical need, communication requirement or other exceptional circumstance, the school will consider reasonable adjustments on an individual basis. Any agreed exception will be formally authorised, documented, proportionate to the identified need and reviewed regularly. An agreed exception does not create a general entitlement to unrestricted device use.

Section 03

ROLES AND RESPONSIBILITIES

Safeguarding first. Acting quickly. Learning continuously.

The safe and appropriate use of mobile and smart technology is a shared responsibility. All members of the school community are expected to use technology responsibly, uphold professional standards and contribute to maintaining a safe environment for pupils, staff and visitors.

The Headteacher has overall responsibility for the implementation, monitoring and review of this policy. This includes ensuring that appropriate procedures are in place, that staff receive suitable guidance and training, and that any significant breaches are managed in accordance with the school's safeguarding, Positive Support, disciplinary and data protection procedures.
The Headteacher may authorise individual exceptions to this policy where there is a legitimate educational, medical, safeguarding or operational need.

The Designated Safeguarding Lead (DSL), supported by Deputy DSLs, is responsible for ensuring that concerns relating to the misuse of mobile or smart technology are managed appropriately as safeguarding matters where necessary.
This includes:

- providing advice and guidance to staff;
- responding to safeguarding concerns involving mobile or smart technology;
- ensuring concerns are recorded and managed in accordance with safeguarding procedures;
- liaising with external agencies where appropriate;
- supporting staff following incidents involving digital technology.

The Senior Leadership Team is responsible for promoting consistent implementation of this policy, supporting staff in its application and ensuring that appropriate action is taken where expectations are not met.

The Governing Board is responsible for ensuring that appropriate policies are in place to support safeguarding, information security and the safe use of technology. Governors will monitor the effectiveness of this policy through the school's safeguarding and governance arrangements.

All staff have a professional responsibility to model safe and appropriate use of mobile and smart technology and to maintain clear professional boundaries at all times.

All staff must:

- comply with this policy and related school policies;
- use school-issued devices where required for professional purposes;
- challenge or report inappropriate use of mobile or smart technology where it may compromise safeguarding or safety;
- protect confidential information at all times;
- report any suspected misuse, loss of data or safeguarding concern immediately to the DSL or a member of the Senior Leadership Team;
- participate in training relating to safeguarding, online safety, data protection and the appropriate use of technology.

All pupils, parents, carers, visitors, contractors and external professionals are expected to comply with this policy whilst on school premises or participating in school activities. Failure to do so may result in appropriate action being taken, including removal from the school site, withdrawal of permission to access school premises or referral to relevant agencies where necessary.

Section 04

STAFF USE OF MOBILE AND SMART TECHNOLOGY

Sharing responsibility. Coordinating effectively. Maintaining safety.

Riverside Bridge School expects all staff to maintain the highest standards of professional conduct when using mobile and smart technology. The use of personal devices must never compromise safeguarding, confidentiality, professional boundaries or the effective supervision of pupils. Staff are expected to model responsible technology use at all times.

Personal mobile phones, smart watches and other personal smart devices must be switched off or set to silent and kept out of sight whilst staff are undertaking duties involving pupils. Personal devices must not be used in classrooms, corridors, playgrounds, dining areas or any location where pupils are present, except where expressly authorised in accordance with this policy.

Personal devices may only be used during designated breaks in staff-only areas or outside the school site. Staff must not use personal mobile or smart devices to:

- communicate directly with pupils or former pupils;
- communicate with parents or carers using personal telephone numbers, messaging applications or social media;
- take photographs, videos or audio recordings of pupils, staff or school activities;
- access, store or process confidential school information;
- upload personal, confidential or special category data to artificial intelligence platforms or other unapproved online services;
- use personal cloud storage or file-sharing applications for school information;
- undertake any activity that could compromise safeguarding, confidentiality or professional boundaries.

Communication with parents and carers must take place only through approved school communication systems, school email accounts, school-issued devices or other authorised communication platforms. Personal contact details must never be shared with pupils or families.

Where photography, video recording or digital documentation is required for educational, therapeutic or safeguarding purposes, only school-approved devices and authorised systems may be used in accordance with the school's Image Use Policy, Data Protection Policy and Online Safety Policy.

The use of artificial intelligence must comply with the school's AI Guidance and Online Safety Policy. Staff must not rely on AI-generated information without appropriate professional oversight and must never enter confidential or personally identifiable information into unapproved AI systems.

In exceptional circumstances, such as a genuine family emergency, significant operational requirement or critical incident, a member of the Senior Leadership Team may authorise temporary use of a personal device. Such authorisation will be proportionate, time limited and must not compromise pupil supervision or safeguarding.

Any accidental recording, photography, data capture or inappropriate access involving a personal device must be reported immediately to the Designated Safeguarding Lead and, where appropriate, the Data Protection Lead. Appropriate action will be taken to secure or remove the material in accordance with safeguarding and data protection procedures.

Failure to comply with this policy may constitute misconduct and will be managed in accordance with the Staff Code of Conduct and the school's disciplinary procedures. Where safeguarding concerns arise, the matter will also be managed in accordance with the Safeguarding and Child Protection Policy.

Section 05

USE OF MOBILE AND SMART TECHNOLOGY DURING OFF-SITE ACTIVITIES

Identifying risk. Strengthening supervision. Preventing incidents.

The expectations set out in this policy apply equally when staff, pupils and volunteers are participating in educational visits, residential visits, community access activities, work-related learning, transport or any other activity organised or supervised by Riverside Bridge School. Safeguarding, confidentiality and professional conduct remain paramount regardless of location.

Staff must ensure that personal mobile and smart devices do not interfere with the supervision of pupils or compromise professional boundaries whilst off-site. Personal devices must not be used in the presence of pupils unless there is an exceptional operational or emergency need and no suitable school-issued device is available.

Where communication, navigation, emergency contact or access to educational resources is required during an off-site activity, staff should use school-issued devices wherever possible.

Staff must not use personal devices to:

- take photographs, video or audio recordings of pupils;
- communicate directly with parents or carers regarding individual pupils;
- share images, videos or information relating to pupils through personal messaging services or social media;
- upload photographs, recordings or confidential information to personal cloud storage or artificial intelligence platforms;
- disclose the location or movements of pupils through social media or other public platforms.

In the event of an emergency, where a school-issued device is unavailable and the use of a personal mobile phone is necessary to protect the safety or welfare of pupils or staff, its use must be limited to the immediate emergency. The circumstances must be reported to a member of the Senior Leadership Team and, where appropriate, the Designated Safeguarding Lead as soon as reasonably practicable.

Where authorised photography or video recording forms part of an educational visit, only school-approved devices may be used, and all images must be managed in accordance with the school's Image Use Policy, Data Protection Policy and Online Safety Policy. Any loss, theft, accidental disclosure of information or safeguarding concern involving mobile or smart technology during an off-site activity must be reported immediately in accordance with the school's safeguarding and data protection procedures.

Failure to comply with this section of the policy may result in disciplinary action and, where appropriate, safeguarding procedures being implemented.

Section 06

USE OF MOBILE AND SMART TECHNOLOGY BY PUPILS

Understanding individual risk. Planning proactively. Promoting safe independence.

Riverside Bridge School recognises that some pupils may own or carry mobile phones or other smart devices for reasons such as independent travel, communication with family, personal safety or medical needs outside school hours. However, to maintain a safe, calm and distraction-free learning environment, the school operates as a mobile-phone-free environment throughout the school day.

Pupils must not use or have access to mobile phones or smart technology with communication, internet, recording or messaging capability during lessons, transitions, breaktimes, lunchtime or any other school-supervised activity unless an individual exception has been formally authorised by the school.

Where a pupil brings a mobile phone or smart device onto the school site, it must be handed to a designated member of staff immediately on arrival. Devices will be securely stored throughout the school day and returned at the end of the school day in accordance with school procedures. Pupils must not keep mobile phones or smart devices on their person, in bags, coats or classrooms during the school day.

Pupils must not use mobile or smart technology to:

- take photographs, videos or audio recordings;
- access the internet or social media;
- send or receive messages or telephone calls;
- record members of staff or other pupils;
- access artificial intelligence applications unless specifically authorised as part of planned learning using approved school systems;
- undertake any activity that compromises safeguarding, privacy or the learning environment.

Where a pupil is found to have retained or used a prohibited device, staff may confiscate the device in accordance with this policy, the school's Positive Support Policy and current Department for Education guidance on searching, screening and confiscation. Parents or carers will normally be informed, and the device will be returned in accordance with school procedures.

Repeated or significant breaches will be considered in the context of the pupil's individual needs and circumstances and may require further Positive Support, safeguarding intervention or work with the pupil and their family.

The school recognises its duties under the Equality Act 2010 and will consider reasonable adjustments where a pupil requires access to a mobile or smart device because of a disability, medical condition, communication need, safeguarding vulnerability or other exceptional circumstance. Each request will be assessed individually in consultation with parents, carers and relevant professionals. Any agreed exception will be formally documented within an individual risk assessment or support plan, include appropriate safeguards, be reviewed regularly and will not create a general entitlement to unrestricted device use.

Where pupils use school-issued digital devices as part of teaching and learning, their use will be supervised by staff and managed in accordance with the school's Online Safety Policy, Acceptable Use Agreements and relevant curriculum procedures.

Section 07

USE OF MOBILE AND SMART TECHNOLOGY BY PARENTS, CARERS, VISITORS AND EXTERNAL PROFESSIONALS

Acting immediately. Searching systematically. Escalating appropriately.

Riverside Bridge School welcomes parents, carers, visitors and external professionals as valued partners in supporting pupils. Everyone attending the school has a shared responsibility to protect the privacy, dignity and safety of pupils, staff and families. The use of mobile and smart technology on the school site must therefore be appropriate, proportionate and consistent with the school's safeguarding expectations. Visitors are expected to keep mobile phones, smart watches and other personal smart devices on silent and out of sight whilst in areas where pupils are present. Mobile devices should only be used where this does not compromise safeguarding, supervision or the privacy of others.

Parents, carers, visitors and external professionals must not:

- take photographs, videos or audio recordings of pupils, staff or school activities without prior authorisation;
- use personal devices in classrooms or other areas where pupils are present unless authorised;
- record conversations or meetings without the prior agreement of everyone involved;
- use social media or messaging applications to share images, information or the location of pupils whilst on the school site;
- use mobile or smart technology in any manner that compromises safeguarding, confidentiality or the smooth operation of the school.

Where a visitor needs to make or receive an urgent telephone call, they should move to a designated area identified by a member of staff where pupils are not present.

External professionals who require digital devices as part of their professional role, for example to complete assessments or access secure records, must seek approval from the Headteacher or an authorised member of staff where appropriate. Any photographs, recordings or information collected must comply with UK GDPR, the Data Protection Act 2018, professional standards and the school's safeguarding procedures.

Contractors working on the school site will be informed of the school's expectations regarding the use of mobile and smart technology during induction or sign-in procedures. Unauthorised photography, video recording or use of personal devices in pupil areas is prohibited.

Tracking Devices

Pupils must not bring or wear personal tracking devices, including AirTags and similar Bluetooth or GPS-enabled devices, unless prior written authorisation has been provided by the Headteacher.

Unauthorised tracking devices may create privacy, safeguarding, security and health and safety risks, including unauthorised location monitoring, surveillance, small-part hazards and the risks associated with button batteries.

Where a family believes a tracking device is necessary because of a pupil's disability, medical need, communication need, travel arrangements or safeguarding vulnerability, the school will consider the request on an individual basis. Where appropriate, a documented risk assessment or individual support plan will be agreed which identifies how the device may be used safely whilst protecting the privacy and safety of all pupils.

Unauthorised drones and remote-controlled devices

The unauthorised use of drones or other remotely operated devices over, within or immediately adjacent to the school site presents potential safeguarding, privacy, security and health and safety risks. Pupils, parents, visitors and members of the public must not operate drones from, over or towards the school site without the prior written permission of the Headteacher.

Where an unauthorised drone is observed, staff must immediately notify a member of the Senior Leadership Team. A dynamic risk assessment will determine the most appropriate response according to the circumstances. This may include:

- moving pupils indoors or away from affected areas;
- restricting access to outdoor spaces;
- implementing lockdown or other emergency procedures where appropriate;
- preserving CCTV or other available evidence;
- contacting the police where criminal activity, significant safeguarding concerns or an immediate threat to safety is suspected;
- informing the Trust, local authority or other relevant agencies where appropriate.

A 999-emergency call will be made where there is an immediate risk to life, serious injury, public safety or the security of the school site.

Failure to comply with the expectations set out in this section may result in an individual being asked to cease using their device, leave the school premises or, where appropriate, further action being taken in accordance with the school's safeguarding procedures, Code of Conduct or relevant legislation.

Section 08

SEARCHING, SCREENING, CONFISCATION AND EXAMINATION OF DEVICES

Recognising high risk. Escalating immediately. Protecting safety.

The school may confiscate mobile phones, smart technology and other electronic devices and, where the statutory conditions are met, authorised staff may search for or examine devices in accordance with current Department for Education guidance on searching, screening and confiscation.

Any search, confiscation or examination will be undertaken lawfully, proportionately and with due regard to the pupil's dignity, welfare, communication needs and individual circumstances. Staff must not search a pupil or examine the contents of an electronic device unless they are authorised to do so and the relevant legal conditions are satisfied.

Where a member of staff becomes aware that a pupil may possess a prohibited item or device presenting a safeguarding or safety concern, they should seek support from an authorised member of staff and follow the school's agreed procedure.

Examination of electronic devices

Where there is good reason to do so, an authorised member of staff may examine data or files stored on an electronic device where this is permitted by law and necessary to:

- investigate a suspected breach of school rules;
- protect the safety or welfare of pupils or staff;
- investigate suspected bullying, harassment or abusive behaviour;
- investigate suspected criminal activity;
- respond to a safeguarding concern.

Staff will only access information that is reasonably necessary for the purpose of the examination and will avoid unnecessary intrusion into personal information.

If, during an examination, staff discover or reasonably suspect that a device contains evidence relating to:

- child sexual abuse material;
- exploitation;
- serious violence;
- criminal activity;
- terrorism;

- or any other safeguarding concern,

the device will be secured immediately and the Designated Safeguarding Lead informed without delay. The school will not intentionally delete or alter material that may be required as evidence and will seek advice from the police or other relevant agencies where appropriate.

Where inappropriate material is identified that does not require police involvement, the school may require relevant files to be deleted where this is lawful and appropriate, in line with current Department for Education guidance.

Staff will not routinely examine electronic devices. Examination will only take place where there is a lawful, proportionate and justified reason to do so, with safeguarding and the welfare of pupils remaining the overriding consideration.

Section 09

ARTIFICIAL INTELLIGENCE (AI) AND EMERGING TECHNOLOGIES

Checking wellbeing. Recording accurately. Learning from incidents.

Riverside Bridge School recognises that artificial intelligence and other emerging technologies may support learning, communication, accessibility and administrative practice but may also create safeguarding, privacy, accuracy, bias and data protection risks.

The use of AI through mobile or smart technology must comply with the school's Artificial Intelligence (AI) Guidance, Online Safety Policy and Data Protection Policy. Personal, confidential or special category information must not be entered into unapproved AI platforms. AI-generated content must be subject to appropriate professional oversight and must not replace professional judgement or safeguarding decision-making.

Pupils may access AI technologies only through approved systems as part of planned and appropriately supervised learning.

The school will keep emerging technologies under review and may introduce additional safeguards where new technologies create safeguarding, privacy, security or data protection risks.

Section 10

LOSS, THEFT, DATA BREACHES AND INCIDENT REPORTING

Reviewing incidents. Identifying patterns. Strengthening practice.

The loss, theft or misuse of mobile and smart technology may present significant safeguarding, operational and data protection risks. All incidents involving school information, personal data or devices used for school purposes must be reported immediately so that appropriate action can be taken to protect individuals and minimise any potential impact.

Any member of staff who becomes aware that a mobile phone, laptop, tablet, smart device, removable media or other device containing school information has been lost, stolen, damaged, compromised or accessed without authorisation must report the matter immediately to their line manager and the school's Data Protection Lead. Where safeguarding concerns are identified, the Designated Safeguarding Lead must also be informed without delay.

Examples of incidents that must be reported include:

- loss or theft of a school-issued device;
- loss or theft of a personal device containing school information;
- unauthorised access to confidential or personal information;
- accidental disclosure or sharing of sensitive information;
- suspected malware, hacking or cyber security incidents involving mobile devices;
- unauthorised photography, video or audio recordings;
- inappropriate use of artificial intelligence involving school information;
- any incident that may compromise safeguarding, confidentiality or the security of the school.

Following notification, the school will take appropriate action, which may include:

- securing or remotely disabling school-issued devices where possible;
- assessing the safeguarding implications;
- investigating the circumstances of the incident;
- implementing measures to reduce further risk;
- notifying the Trust and relevant senior leaders;

- reporting personal data breaches in accordance with the school's Data Protection Policy and UK GDPR requirements;
- referring matters to the police or other external agencies where appropriate.

Staff must not attempt to conceal, delay reporting or independently investigate incidents involving lost devices or potential data breaches. Prompt reporting enables the school to fulfil its legal safeguarding and data protection responsibilities and minimise potential harm.

Where an incident involves personal data, the school will assess whether it constitutes a personal data breach and will manage the incident in accordance with UK GDPR, the Data Protection Act 2018 and the school's Data Protection Policy.

Where lessons can be learned from an incident, these will be incorporated into staff training, risk assessments and future policy reviews to strengthen safeguarding and information security arrangements.

Section 11

MONITORING, COMPLIANCE AND REVIEW

Monitoring practice. Maintaining compliance. Responding to change.

Riverside Bridge School is committed to ensuring that this policy is implemented consistently and remains effective in protecting pupils, staff and the wider school community. Compliance with this policy forms part of the school's wider safeguarding, information security and professional conduct arrangements.

The school may monitor the use of school-issued devices, networks, internet services and digital systems where this is lawful, proportionate and necessary for safeguarding, security, operational management or compliance with legal obligations. Monitoring will be undertaken in accordance with UK GDPR, the Data Protection Act 2018, the Investigatory Powers Act 2016, the school's Data Protection Policy and relevant Department for Education guidance.

Use of school-owned devices, networks and digital systems may be monitored where this is lawful, necessary, proportionate and transparent. Monitoring will only be undertaken by authorised personnel for legitimate safeguarding, security, operational or legal purposes.

Concerns regarding inappropriate use of mobile or smart technology will be considered under the appropriate safeguarding, pupil support, professional conduct, disciplinary, online safety or data protection procedures, according to the nature and circumstances of the concern.

Where breaches of this policy involve safeguarding concerns, criminal offences or significant data protection issues, the school may involve external agencies, including the police, children's social care, the Local Authority Designated Officer (LADO), the Information Commissioner's Office (ICO) or other appropriate organisations.

This policy will be reviewed annually, or sooner if required following:

- changes to legislation or statutory guidance;
- updates to Department for Education guidance;
- developments in mobile, smart or emerging technologies;
- safeguarding or data protection incidents;
- recommendations arising from audits or inspections;
- changes to school practice or organisational structure.

The Headteacher has overall responsibility for ensuring that this policy remains current and effective. Governors will receive appropriate assurance that the policy is being implemented and reviewed as part of the school's wider safeguarding and governance arrangements.

Section 12

RELATED POLICIES & FRAMEWORKS

Connecting practice. Strengthening consistency.

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Online Safety Policy
- Positive Support Policy
- Staff Code of Conduct
- Data Protection Policy
- Educational Visits Policy
- Risk Assessment Policy
- Disciplinary Policy
- Acceptable Use Agreements
- Emergency Management and Business Continuity Plan
- Lockdown Policy.