ONLINE SAFETY POLICY

Using technology safely. Building understanding.
Protecting pupils.



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 online safety. It explains the principles, expectations, responsibilities and arrangements through which the school enables pupils to benefit from digital technology while protecting them from online harm, maintaining safe and secure systems and developing the knowledge, communication and practical skills required to participate safely in an increasingly digital world.

At Riverside Bridge School, online safety is an integral part of safeguarding and underpins the safe use of technology across teaching, learning, communication and wider school life. Technology can provide significant opportunities for pupils to communicate, access learning, exercise choice, develop independence and participate more fully in their communities. At the same time, digital technologies can expose pupils to risks that require effective education, appropriate supervision, strong safeguarding practice and proportionate technical safeguards.

As a specialist school, we recognise that online risk must be understood in the context of the individual pupil. Communication differences, cognitive and developmental needs, sensory processing, social understanding, emotional regulation and varying levels of independence may affect how pupils recognise risk, understand online interactions, communicate concerns or respond when something feels unsafe. Online safety education and safeguarding responses must therefore be personalised and accessible rather than based solely upon chronological age.

Our approach is preventative and enabling. Filtering, monitoring and cyber security provide important safeguards, but they do not replace high-quality teaching, professional curiosity, trusted relationships or accessible communication. Pupils should be supported progressively to recognise risk, communicate discomfort or concern, seek help from trusted adults, protect personal information and use technology with increasing safety and independence.

Online safety is embedded across the curriculum and wider school experience rather than treated as a single lesson or programme. Through Computing, PSHE/RSE and Health Education, communication, preparation for adulthood and everyday use of technology, pupils encounter online safety learning in ways that are meaningful to their lives and appropriate to their developmental profiles.

The school also recognises that technology evolves rapidly. Artificial intelligence, social media, connected devices, online communication and emerging digital platforms continue to create both opportunities and new safeguarding considerations. Riverside Bridge School therefore maintains a responsive approach in which policy, education, technical controls and staff knowledge are reviewed as technologies and risks develop.

Where an online concern arises, the welfare of the pupil remains paramount. Staff must respond promptly, preserve relevant information where appropriate and report safeguarding concerns without delay. Staff are not expected to investigate safeguarding concerns themselves; concerns are managed through the school's established safeguarding procedures and escalated to external agencies where required.

Our responsibilities to pupils, families and the school community

Riverside Bridge School has a responsibility to provide a safe digital environment in which pupils can access the benefits of technology while receiving appropriate protection, education and support.

In delivering this responsibility, we will:

- place safeguarding at the centre of decisions relating to digital technology and online activity;
- provide age- and developmentally appropriate online safety education personalised to pupils' communication and learning needs;
- maintain effective and proportionate filtering, monitoring and cyber security arrangements;
- ensure pupils have accessible ways to communicate when something online causes concern, confusion, discomfort or distress;
- support pupils to develop increasing understanding, agency and independence in their use of technology;
- maintain appropriate supervision while recognising that technical controls cannot eliminate all online risk;
- ensure staff understand their responsibilities for professional conduct, information security and safeguarding when using technology;
- maintain clear expectations for the use of mobile devices, digital images, social media, artificial intelligence and school systems;
- protect personal, confidential and safeguarding information in accordance with data protection requirements;
- respond promptly and proportionately to online safety concerns and incidents;
- work collaboratively with parents and carers to strengthen safe technology use beyond the school day;
- work with technical providers and safeguarding partners where specialist advice or intervention is required; and
- regularly review online safety arrangements in response to incidents, emerging technologies, statutory guidance and identified risks.

Through these commitments, we aim to ensure that every pupil can participate in the digital world as safely, confidently and independently as possible, while being protected from harm and supported to communicate when they need help.

TABLE OF CONTENTS

01	ONLINE SAFETY AT RIVERSIDE BRIDGE SCHOOL	02	LEGISLATIVE AND STATUTORY FRAMEWORK
03	PRINCIPLES	04	LEADERSHIP, GOVERNANCE AND RESPONSIBILITIES
05	FILTERING, MONITORING AND CYBER SECURITY	06	ONLINE SAFETY EDUCATION
07	ARTIFICIAL INTELLIGENCE (AI)	08	MOBILE DEVICES AND SMART TECHNOLOGY
09	ACCEPTABLE USE OF TECHNOLOGY	10	DIGITAL IMAGES, PHOTOGRAPHY, VIDEO RECORDING AND LIVE STREAMING
11	SOCIAL MEDIA	12	ONLINE RISKS AND SAFEGUARDING
13	MANAGING ONLINE SAFETY INCIDENTS	14	REMOTE LEARNING, EDUCATIONAL VISITS AND OFF-SITE ACTIVITIES
15	MONITORING, REVIEW AND GOVERNANCE	16	RELATED POLICIES AND FRAMEWORKS
	APPENDICES		

APPROVED BY: Governing Board

APPROVED ON: September 2026

REVIEWED DUE ON: September 2027

Section 01

ONLINE SAFETY AT RIVERSIDE BRIDGE SCHOOL

Enabling access. Developing understanding. Protecting pupils.

1.1 School approach

Online safety is an integral part of safeguarding at Riverside Bridge School and is embedded across teaching, learning, communication and wider school life. Technology provides important opportunities for pupils to access learning, communicate, make choices, develop interests and participate with increasing independence in school, at home and within the wider community.

Our approach recognises that safe use of technology requires more than technical protection. Effective online safety combines accessible education, appropriate supervision, positive relationships, professional curiosity, secure digital systems and clear safeguarding procedures.

As a specialist school, we recognise that pupils may experience online opportunities and risks differently according to their communication, cognitive, sensory, physical and developmental profiles. Expectations, teaching and support are therefore personalised to the individual pupil, enabling access to technology while providing the level of protection, guidance and supervision they require.

Online safety is not treated as a standalone area of practice. Pupils are supported progressively to develop the understanding and practical skills needed to use technology safely, communicate concerns, seek support from trusted adults and participate in the digital world with increasing confidence and independence.

1.2 Scope

This policy applies to all members of the Riverside Bridge School community, including pupils, staff, governors, volunteers, agency staff, contractors, visitors and professionals working on behalf of the school.

The policy applies whenever school technologies, digital systems or online services are used, whether on the school site, during educational visits, while working remotely or in any other context connected with school activities.

It also applies where online activity outside school presents a safeguarding concern, affects the welfare of a pupil or member of staff, or has the potential to impact upon the safe and effective operation of the school.

1.3 Relationship with wider school practice

Online safety forms part of Riverside Bridge School's wider approach to safeguarding, curriculum, communication, Positive Support, information governance and professional conduct. It is embedded within everyday practice rather than operating as a separate system or responsibility.

The school's Total Communication approach supports pupils to understand information, express choices and communicate concerns in ways that are accessible to them. Positive Support promotes understanding of individual need, regulation and safe participation, while curriculum learning progressively develops pupils' knowledge and skills for using technology safely and with increasing independence.

Online safety also operates alongside the school's safeguarding, data protection, information security and professional conduct arrangements. Staff must therefore consider online concerns within the pupil's wider context and follow the relevant safeguarding, reporting and information-sharing procedures where concerns arise.

This policy forms part of the school's wider safeguarding and digital governance arrangements and should be read alongside the related policies and frameworks identified in Section 16.

Section 02

LEGISLATIVE AND STATUTORY FRAMEWORK

Understanding duties. Applying guidance. Maintaining safeguards.

Riverside Bridge School has developed this policy in accordance with current legislation, statutory guidance and recognised national best practice relating to safeguarding, online safety, data protection and the safe use of digital technologies.

The school recognises that online safety is an integral part of its safeguarding responsibilities and that effective online safety arrangements require a whole-school approach involving leadership, governance, education, technology and partnership working with families.

This policy should be read alongside current statutory guidance and is informed by, but not limited to, the following:

- Keeping Children Safe in Education (Department for Education, current edition);
- Working Together to Safeguard Children (HM Government, current edition);
- Education Act 2002;
- Children Act 1989 and Children Act 2004;
- Online Safety Act 2023;
- Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR);
- Human Rights Act 1998;
- Equality Act 2010;
- Counter-Terrorism and Security Act 2015 (Prevent Duty);
- Searching, Screening and Confiscation (Department for Education, current edition);
- Meeting Digital and Technology Standards in Schools and Colleges: Filtering and Monitoring Standards (Department for Education, current edition);
- Cyber Security Standards for Schools and Colleges (Department for Education, current edition);
- Generative Artificial Intelligence in Education guidance published by the Department for Education and other recognised national bodies, where applicable.

The school also takes account of guidance published by the UK Safer Internet Centre, National Cyber Security Centre (NCSC), Child Exploitation and Online Protection (CEOP), Internet Watch Foundation (IWF), Ofcom and other recognised organisations where this supports the implementation of safe practice.

Online safety arrangements will be reviewed regularly to ensure that they remain consistent with changes in legislation, statutory guidance, emerging technologies and identified safeguarding risks.

Section 03

PRINCIPLES

Prioritising safeguarding. Enabling participation. Building independence.

Online safety at Riverside Bridge School is based upon the principle that safeguarding is everyone's responsibility. Technology is an essential part of modern life and plays a significant role in education, communication, independence and preparation for adulthood. The school therefore seeks to create an environment where pupils can benefit from technology safely whilst being protected from foreseeable risks. The school recognises that online safety cannot be achieved solely through technical controls such as filtering and monitoring. Effective online safeguarding requires a whole-school approach which combines appropriate leadership, high-quality teaching, clear expectations, robust safeguarding procedures, effective information security and positive partnerships with parents, carers and external agencies.

As a specialist school, Riverside Bridge School recognises that many pupils experience additional vulnerabilities when accessing technology. Communication differences, learning needs, sensory processing differences, social understanding and varying levels of independence may increase a pupil's vulnerability to online harm. Online safety education and safeguarding responses will therefore be personalised to reflect each pupil's communication, cognitive, developmental and emotional needs.

The school adopts a preventative approach to online safety. Wherever possible, pupils will be supported to develop the knowledge, understanding and practical skills needed to recognise risk, communicate concerns, seek support from trusted adults and use technology safely within school, at home and within the wider community. When responding to online safety concerns, Riverside Bridge School will always place the welfare of the child at the centre of decision-making. Concerns will be managed in accordance with the school's Child Protection and Safeguarding Policy, recognising that online incidents frequently form part of wider safeguarding concerns and may require multi-agency involvement.

The school's approach is underpinned by the following principles:

- safeguarding remains the primary consideration in all decisions relating to technology;
- online safety is embedded throughout the curriculum and daily school practice rather than taught as a standalone topic;
- education, communication and positive relationships are the most effective means of reducing online risk;
- filtering, monitoring and cyber security arrangements support, but do not replace, professional curiosity and effective safeguarding practice;
- pupils, families and staff work together to promote safe, respectful and responsible use of technology;
- online safety arrangements are reviewed regularly to reflect changes in legislation, technology and emerging safeguarding risks.

Section 04

LEADERSHIP, GOVERNANCE & RESPONSIBILITIES

Sharing responsibility. Maintaining oversight. Strengthening safeguards.

Effective online safety requires a whole-school approach. While specific responsibilities are allocated to designated individuals, safeguarding remains the responsibility of every member of the Riverside Bridge School community. All adults are expected to contribute to a culture in which technology is used safely, responsibly and in the best interests of pupils.

The Governing Board and Headteacher retain overall responsibility for ensuring that appropriate arrangements are in place to safeguard pupils online. Day-to-day implementation is led through the school's safeguarding systems, supported by technical expertise, staff training and robust reporting procedures.

Governing Board

The Governing Board has strategic responsibility for ensuring that Riverside Bridge School fulfils its statutory duties relating to online safety and safeguarding.

Governors will seek appropriate assurance that effective systems are in place to protect pupils from online harm and that these arrangements remain effective as technology and safeguarding risks evolve.

In fulfilling this responsibility, the Governing Board will:

- ensure appropriate online safety policies are in place and reviewed regularly;
- receive appropriate assurance regarding filtering, monitoring and cyber security arrangements;
- ensure sufficient resources are available to maintain safe digital systems;
- monitor safeguarding trends, significant online incidents and emerging risks through governance reporting;
- ensure staff receive appropriate training to fulfil their responsibilities;
- support a culture of continuous improvement in online safety across the school.

Headteacher

The Headteacher has overall operational responsibility for the implementation of this policy and for ensuring that online safety forms an integral part of the school's safeguarding culture.

The Headteacher will ensure that:

- effective safeguarding procedures are implemented consistently;
- appropriate filtering, monitoring and cyber security arrangements are maintained;
- staff receive regular online safety training;

- appropriate action is taken where online safety concerns arise;
- sufficient resources are available to support safe use of technology;
- governors receive appropriate reports regarding online safety.

Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) has lead responsibility for safeguarding concerns arising from the use of technology and online services.

The DSL will:

- oversee the management of online safeguarding concerns;
- ensure concerns are recorded, assessed and responded to in accordance with safeguarding procedures;
- work with technical staff where filtering or monitoring identifies safeguarding concerns;
- contribute to staff training and safeguarding updates;
- liaise with parents, carers, external agencies and partner organisations where appropriate;
- monitor emerging safeguarding risks and ensure appropriate responses are developed.

The DSL does not manage the school's technical infrastructure but works closely with those responsible for digital systems to ensure that safeguarding and technical arrangements operate effectively together.

Senior Leadership Team

The Senior Leadership Team will promote a positive culture of safe technology use throughout the school and ensure that online safety is reflected within curriculum development, staff supervision, quality assurance and safeguarding practice.

Senior leaders will support staff in implementing this policy, monitor compliance within their areas of responsibility and ensure that concerns are escalated promptly where necessary.

Staff

Every member of staff has a responsibility to safeguard pupils when using technology and to promote safe, responsible and respectful use of technology.

All staff are expected to:

- model safe and professional use of technology;
- follow the school's acceptable use expectations;
- maintain appropriate professional boundaries online;
- recognise and report online safeguarding concerns without delay;
- participate in required online safety and safeguarding training;
- use school technology in accordance with information security requirements.

Staff must never assume that filtering or monitoring systems alone will identify all safeguarding concerns and should always exercise professional curiosity and judgement.

Technical Support and IT Providers

The school works with its technical support provider to maintain secure digital systems which support teaching, learning and safeguarding.

Those responsible for technical services will:

- maintain appropriate filtering and monitoring systems;
- implement security updates and patches promptly;
- investigate technical concerns relating to online safety;
- support cyber security arrangements;
- advise school leaders regarding emerging technical risks;
- work with safeguarding leaders where monitoring identifies potential concerns.

Technical staff do not make safeguarding decisions but will work collaboratively with school leaders when concerns arise.

Pupils

Pupils are encouraged to use technology safely, respectfully and responsibly. Expectations will be taught in ways that are appropriate to each pupil's age, stage of development, communication profile and level of understanding.

Pupils will be supported to:

- communicate if something online makes them feel worried, upset or unsafe;
- seek help from trusted adults;
- respect others when using technology;
- use school technology in accordance with staff guidance;
- develop increasing independence in using technology safely as part of preparation for adulthood.

Parents and Carers

The school recognises that parents and carers play a vital role in promoting online safety beyond the school day. Riverside Bridge School will work in partnership with families by providing advice, guidance and support where appropriate, sharing information about emerging online risks and encouraging consistent messages regarding safe and responsible use of technology.

Parents and carers are encouraged to communicate any online safety concerns that may affect a pupil's welfare so that the school can provide appropriate support and, where necessary, work collaboratively with other agencies.

Section 05

FILTERING, MONITORING AND CYBER SECURITY

Reducing risk. Identifying concerns. Protecting systems.

Riverside Bridge School recognises that effective online safety relies upon a combination of appropriate technical controls, secure digital systems and informed professional judgement. Filtering and monitoring systems are an important safeguarding measure, but they cannot identify every risk or replace the vigilance of staff.

The school maintains proportionate filtering, monitoring and cyber security arrangements which are appropriate to the age, needs and vulnerabilities of its pupils. These arrangements are reviewed regularly to ensure that they remain effective, support learning and reflect current safeguarding risks.

5.1 Filtering

Internet filtering systems are used to reduce the likelihood of pupils and staff accessing illegal, harmful or inappropriate online content whilst enabling access to educational resources necessary for teaching and learning.

Filtering arrangements are designed to:

- protect pupils from harmful and inappropriate online material;
- minimise exposure to illegal or extremist content;
- support the delivery of the curriculum;
- provide age- and needs-appropriate access to online resources;
- allow legitimate educational access where appropriate.

The school recognises that filtering systems cannot remove all online risk and that some safeguarding concerns may arise through content that is not blocked. Staff therefore remain responsible for supervising pupils appropriately and responding to any concerns that arise.

Where legitimate educational resources are inadvertently blocked, staff should report this through the school's agreed technical support procedures so that access can be reviewed where appropriate.

5.2 Monitoring

Monitoring systems are used to identify activity which may indicate a safeguarding concern, misuse of school technology or a potential cyber security incident.

Monitoring may identify concerns including, but not limited to:

- attempts to access inappropriate content;

- unsafe or concerning online searches;
- indicators of self-harm or suicidal ideation;
- bullying, harassment or discriminatory language;
- potential child-on-child abuse;
- attempts to bypass filtering systems;
- activity which may indicate online grooming, exploitation or radicalisation;
- activity which may present a cyber security risk to the school.

Monitoring alerts are reviewed by appropriate members of staff in accordance with the school's safeguarding procedures. Where an alert indicates that a pupil may be at risk of harm, the concern will be referred immediately to the Designated Safeguarding Lead and managed in line with the Child Protection and Safeguarding Policy.

Monitoring information is treated confidentially and accessed only by authorised personnel for safeguarding, security and operational purposes.

5.3 Cyber security

The school is committed to maintaining secure digital systems that protect pupils, staff and sensitive information from cyber threats. Appropriate measures are implemented to reduce the risk of unauthorised access, data loss and disruption to school systems. These include secure user authentication, regular software updates, anti-malware protection, secure backup arrangements and appropriate management of user accounts and permissions. All members of staff have a responsibility to support cyber security by:

- using strong, secure passwords and protecting login credentials;
- following school procedures for accessing digital systems;
- reporting suspected phishing emails or cyber incidents immediately;
- ensuring school devices are used appropriately and securely;
- protecting confidential and personal information in accordance with the Data Protection Policy;
- locking devices when left unattended and storing portable equipment securely.

Any suspected cyber security incident, attempted breach or compromise of school systems must be reported immediately through the school's reporting procedures so that appropriate action can be taken.

5.4 Review of technical safeguards

Filtering, monitoring and cyber security arrangements are reviewed regularly by school leaders in collaboration with the school's technical support provider. Reviews consider the effectiveness of existing controls, emerging safeguarding risks, curriculum requirements and any incidents or trends identified through safeguarding or technical monitoring.

The Governing Board receives appropriate assurance that these arrangements remain effective and continue to meet statutory expectations.

Section 06

ONLINE SAFETY EDUCATION

Building knowledge. Developing skills. Increasing independence.

Riverside Bridge School believes that the most effective way to protect pupils online is through high-quality education, supported by appropriate supervision and positive relationships. Online safety is therefore taught as part of the school's wider safeguarding curriculum and is reinforced through everyday teaching, communication and interactions across the school.
Given the diverse needs of our pupils, online safety education is carefully adapted to reflect individual communication, cognitive, sensory and developmental profiles.

The school recognises that pupils will access technology in different ways and may require varying levels of support to understand online risks, develop safe online activities and apply their learning in different contexts.
Online safety is not delivered as a single programme or isolated lesson. It is embedded across the curriculum and revisited regularly to ensure that learning is meaningful, progressive and relevant to pupils' everyday experiences.

6.1 Curriculum provision

Online safety education is delivered through a range of curriculum areas, including Computing, Personal, Social, Health and Economic (PSHE) Education, Relationships Education, Relationships and Sex Education (RSE), communication programmes and Preparation for Adulthood learning.
Teaching is designed to develop pupils' understanding of:

- using technology safely and responsibly;
- recognising trusted adults and knowing how to seek help;
- respecting others when communicating online;
- protecting personal information;
- recognising unsafe situations or inappropriate online activity;
- understanding that not everything seen online is accurate or trustworthy;
- developing safe habits when using digital devices;
- making positive choices when accessing online content and services.

Learning is delivered using approaches appropriate to individual pupils, including visual supports, structured teaching, modelling, repetition, social stories, symbols, role play, communication systems and practical activities where appropriate.

6.2 Personalised learning

The school recognises that online safety learning will look different across the four curriculum pathways. Expectations are matched to each pupil's stage of development, communication abilities and level of independence rather than chronological age alone.

For some pupils, learning may focus on recognising familiar adults, requesting help and understanding simple safety routines when using technology. For others, it may include managing online relationships, understanding privacy, recognising manipulation or misinformation, using social media responsibly and developing the skills required for independent participation in an increasingly digital society.

Where appropriate, online safety targets may be incorporated into individual learning programmes, communication targets or Preparation for Adulthood outcomes.

6.3 Working with parents and carers

The school recognises that effective online safety extends beyond the school day and that parents and carers have an essential role in supporting children to use technology safely.

Riverside Bridge School will work in partnership with families by:

- providing information about emerging online risks where appropriate;
- sharing advice on safe use of technology within the home;
- signposting families to reliable sources of guidance and support;
- discussing online safety as part of wider safeguarding conversations where relevant;
- encouraging parents and carers to communicate any concerns that may affect a pupil's wellbeing or safety.

The school acknowledges that technology develops rapidly and that families may require ongoing support to understand new platforms, applications and digital risks. Wherever possible, information shared with parents and carers will be practical, accessible and relevant to the needs of Riverside pupils.

6.4 Staff training

All staff receive appropriate safeguarding and online safety training as part of their induction and ongoing professional development.

Training is reviewed regularly to reflect changes in legislation, emerging technologies and current safeguarding risks. This may include updates relating to artificial intelligence, cyber security, online exploitation, harmful online activity, filtering and monitoring arrangements and local safeguarding concerns.

Staff are expected to maintain an awareness of current online safety issues and to apply this knowledge consistently within their professional practice.

Section 07

ARTIFICIAL INTELLIGENCE (AI)

Using AI responsibly. Protecting information. Maintaining oversight.

Artificial intelligence (AI) is becoming an increasingly common part of education and everyday life. Riverside Bridge School recognises that AI technologies can provide valuable opportunities to support learning, communication, accessibility, creativity and administrative efficiency. At the same time, AI presents new safeguarding, ethical and information security considerations which require careful management.

The school will ensure that the use of AI supports learning and professional practice whilst maintaining the highest standards of safeguarding, confidentiality, data protection and professional integrity.

The use of AI within Riverside Bridge School will always be proportionate, transparent and subject to appropriate professional oversight. AI will support, but never replace, professional judgement, safeguarding decision-making or direct teaching.

7.1 Use of Artificial Intelligence

Where AI technologies are used within the school, they will be implemented in a manner that:

- supports teaching, learning and accessibility where educationally appropriate;
- protects personal and confidential information;
- complies with UK GDPR and the Data Protection Act 2018;
- promotes safe and ethical use of technology;
- is appropriate to the age, understanding and individual needs of pupils;
- is subject to appropriate staff supervision.

The school will assess emerging AI technologies before they are introduced to ensure that any safeguarding, privacy or security risks have been appropriately considered.

7.2 Staff responsibilities

Staff may use approved AI technologies to support professional practice where this is appropriate and consistent with school policies.

When using AI, staff must:

- exercise professional judgement at all times;
- verify the accuracy of AI-generated information before relying upon it;
- protect confidential, personal and safeguarding information;
- avoid entering identifiable pupil, staff or family information into unauthorised AI systems;

- ensure that AI-generated materials are appropriate, accurate and inclusive before use with pupils;
- follow the school's Artificial Intelligence Policy and Data Protection Policy.

AI-generated content must never replace professional assessment, safeguarding decision-making, statutory reporting or other responsibilities that require human judgement. Staff should also recognise that publicly available photographs and videos may be copied, manipulated or incorporated into artificial intelligence systems beyond the school's control. This potential risk should be considered when deciding whether the publication of images is necessary, proportionate and in the best interests of the pupil.

7.3 Teaching pupils About AI

Where appropriate to pupils' age, developmental stage and communication needs, the curriculum will introduce basic concepts relating to artificial intelligence and responsible technology use.

Pupils may be supported to understand that:

- AI-generated information may not always be accurate;
- images, videos and audio can be created or altered using AI;
- not everything seen online should be believed without question;
- trusted adults should be asked for help if something online causes confusion or concern;
- technology should be used safely, respectfully and responsibly.

Teaching will always be adapted to meet individual learning needs and will reflect the school's personalised curriculum.

7.4 Further guidance

Detailed expectations relating to the educational, professional and administrative use of artificial intelligence are set out within the school's Artificial Intelligence Policy. Any safeguarding concerns arising from the use of AI will be managed in accordance with the Child Protection and Safeguarding Policy.

Section 08

MOBILE DEVICES AND SMART TECHNOLOGY

Managing access. Protecting privacy. Supporting safe use.

Digital devices, including mobile phones, tablets, smart watches and other internet-enabled technologies, form an increasingly important part of everyday life. Riverside Bridge School recognises that these technologies can support communication, accessibility and learning when used appropriately. However, they also present safeguarding, privacy and information security risks which require clear expectations and effective management.

The school is committed to maintaining a safe learning environment in which the use of mobile devices and smart technology supports education and safeguarding without disrupting learning or compromising the welfare of pupils, staff or visitors.

The management of mobile phones, personal devices, wearable technology and other smart devices is set out in the school's Mobile and Smart Technology Policy, which should be read alongside this policy.

8.1 School expectations

All members of the school community are expected to use digital devices responsibly and in accordance with school procedures.

This includes:

- using technology only for appropriate educational or professional purposes;
- protecting the privacy and dignity of pupils, staff and visitors;
- complying with safeguarding, confidentiality and data protection requirements;
- following staff instructions regarding the use of personal devices within school;
- reporting the loss, theft or suspected misuse of any school device without delay.

Unauthorised photography, audio recording or video recording of pupils, staff or visitors is not permitted unless authorised for educational, safeguarding or operational purposes and undertaken in accordance with school procedures.

8.2 Pupils

Pupils are not permitted to access personal mobile phones or personal internet-enabled devices during the school day unless this has been specifically authorised as part of an individual risk assessment, healthcare plan, communication provision or other agreed educational arrangement.

Where a pupil brings a mobile phone or other personal smart device to school, it will be managed in accordance with the school's Mobile and Smart Technology Policy.

Reasonable adjustments will be made where the use of a personal device forms part of an agreed provision to meet a pupil's disability, communication or medical needs.

8.3 Staff

Staff are expected to model safe and professional use of technology at all times.

Personal devices must not be used in the presence of pupils except where this is authorised for school business or in an emergency. Staff must not use personal devices to photograph or record pupils unless this has been specifically authorised and carried out in accordance with school procedures.

Communication with pupils must only take place through approved school systems. Staff must not use personal social media accounts, messaging applications or private email accounts to communicate with pupils.

8.4 Visitors and contractors

Visitors, volunteers, agency staff and contractors are expected to comply with the school's procedures regarding the use of mobile devices whilst on site. Where required, individuals may be asked to refrain from using personal devices in areas where pupils are present or where safeguarding, privacy or confidentiality could be compromised.

Section 09

ACCEPTABLE USE OF TECHNOLOGY

Using technology responsibly. Maintaining boundaries. Protecting others.

Riverside Bridge School expects all members of the school community to use digital technologies safely, responsibly and professionally. Appropriate use of technology supports learning, communication and the effective operation of the school. Inappropriate use may place pupils, staff or the wider school community at risk and may result in disciplinary or safeguarding action.
All users of school technology are expected to act lawfully, respectfully and in accordance with this policy, the school's safeguarding procedures and any relevant acceptable use agreements.

9.1 General expectations

All users of school devices, networks and online services are expected to:

- use technology in a manner that is safe, respectful and appropriate;
- protect passwords and login credentials from unauthorised access;
- safeguard confidential and personal information;
- access only those systems and information required for their role or learning;
- report any safeguarding, security or technical concerns promptly;
- comply with copyright, licensing and intellectual property requirements;
- use school equipment with reasonable care and report any damage or faults.

Technology must never be used in a way that places another person at risk, disrupts learning or brings the school into disrepute.

9.2 Staff expectations

Staff are expected to demonstrate professional standards at all times when using digital technology.
This includes:

- using school-issued accounts and approved systems for school business;
- maintaining appropriate professional boundaries when communicating electronically;
- protecting confidential information in accordance with the Data Protection Policy;
- ensuring electronic communications are professional, appropriate and capable of public scrutiny;
- reporting safeguarding concerns immediately in line with the Child Protection and Safeguarding Policy;
- complying with the Staff Code of Conduct, Mobile and Smart Technology Policy and Artificial Intelligence Policy.

Staff must not:

- access, create, store or distribute inappropriate or illegal material using school systems;
- use school technology for unlawful, discriminatory or offensive purposes;
- bypass security, filtering or monitoring systems;
- share passwords or user accounts;
- install unauthorised software or applications on school devices;
- use personal email accounts or messaging platforms to communicate with pupils.

9.3 Pupil expectations

Pupils will be supported to use technology safely and responsibly in ways that reflect their age, developmental stage and individual needs. With appropriate support, pupils will be encouraged to follow adult instructions when using technology; treat equipment with care; respect the privacy and feelings of others; ask for help if something online makes them feel worried, upset or confused; and use technology for learning, communication and other agreed activities.

Expectations will be taught through the curriculum and reinforced through daily practice using communication methods appropriate to each pupil.

9.4 Visitors, volunteers and contractors

Visitors, volunteers, agency staff, students and contractors are expected to comply with the school's safeguarding procedures and technology expectations whilst on site or when accessing school systems.

Access to school networks or digital systems will be provided only where necessary and will be appropriate to the individual's role. Any concerns regarding misuse of technology must be reported immediately to a member of the Senior Leadership Team or the Designated Safeguarding Lead.

9.5 Breaches of acceptable use

Any suspected misuse of technology will be investigated proportionately and managed in accordance with the school's safeguarding procedures and relevant employment or positive support procedures, as appropriate. Where appropriate, breaches may result in:

- temporary or permanent restriction of access to school technology;
- additional education or support;
- disciplinary action;
- referral through safeguarding procedures;
- involvement of external agencies, including the police, where unlawful activity is suspected.

The school will always consider the age, understanding, communication needs and individual circumstances of the pupil or adult involved when determining an appropriate response.

Section 10

DIGITAL IMAGES, PHOTOGRAPHY, VIDEO RECORDING AND LIVE STREAMING

Protecting dignity. Managing consent. Sharing safely.

The use of photographs, video recordings and other digital media plays an important role in celebrating achievement, supporting learning, evidencing progress and facilitating communication with families. Riverside Bridge School is committed to ensuring that all images and recordings are created, stored and shared in a manner that protects the privacy, dignity and safety of pupils, staff and visitors.

All images and recordings will be managed in accordance with safeguarding requirements, data protection legislation and the school's procedures for the safe use of technology. The welfare of the child will always be the primary consideration when deciding whether photographs or recordings should be taken, retained or shared.

10.1 Educational use

Photographs and video recordings may be taken where they support educational provision, assessment, communication, therapeutic programmes or the wider life of the school.

This may include:

- recording learning and achievement;
- evidencing progress towards individual outcomes;
- supporting communication with parents and carers;
- contributing to assessment and moderation;
- celebrating school activities and events;
- supporting staff training where appropriate.

All recordings must have a clear educational, safeguarding or operational purpose.

10.2 Consent and publication

The school will obtain and manage consent for the use of photographs and recordings in accordance with data protection legislation and the school's published procedures.

Where images are used for publicity, the school website, social media or other external publications, only appropriately authorised images will be used.

Care will be taken to ensure that published material does not unnecessarily identify individual pupils or place them at increased risk.

While parental consent is an important requirement for the use of pupil images, consent alone does not automatically make publication appropriate. Before publishing photographs or videos on the school's website, social media or other public-facing platforms, the school will consider whether identifying the pupil is necessary for the purpose of the communication. Where the same objective can reasonably be achieved using a less identifiable image, this will normally be the preferred approach. Decisions regarding publication will always take account of safeguarding, privacy, dignity and the individual needs of the pupil.

Safer photography practice

Wherever reasonably practicable, photographs published externally should celebrate learning and school life whilst minimising unnecessary identification of pupils.

Wherever appropriate, staff should consider using:

- wider classroom or outdoor scenes;
- photographs taken from behind or over the shoulder;
- hands-on learning activities;
- displays of work or resources where personal information is not visible;
- group activities where no individual pupil is unnecessarily highlighted.

Close-up photographs clearly identifying individual pupils should only be used where there is a clear educational, promotional or celebratory purpose and publication remains appropriate following safeguarding consideration.

10.3 Storage and security

Digital images and recordings created for school purposes must be stored securely using approved school systems.

Staff must not retain photographs or recordings of pupils on personal devices, personal cloud storage or personal online accounts.

Images will be retained only for as long as there is a legitimate educational, safeguarding or operational reason and will be deleted securely when no longer required.

10.4 Live streaming and video communication

Where live streaming, video conferencing or virtual learning platforms are used, appropriate safeguarding measures will be implemented to protect pupils and staff.

Only approved platforms should be used for school purposes. Staff must ensure that online sessions are conducted professionally, that appropriate privacy settings are applied and that pupils are appropriately supervised. Recording of live sessions should only take place where there is a clear educational or operational reason and in accordance with school procedures.

10.5 Personal recording

To protect the privacy and dignity of all members of the school community, unauthorised photography, audio recording or video recording is not permitted on the school site.

This applies equally to pupils, staff, parents, carers, visitors and contractors unless specific authorisation has been provided by the school.

Where concerns arise regarding unauthorised recording, appropriate action will be taken in accordance with the school's safeguarding procedures, Data Protection Policy and Mobile and Smart Technology Policy.

Section 11

SOCIAL MEDIA

Maintaining boundaries. Protecting privacy. Communicating responsibly.

Social media provides valuable opportunities for communication, collaboration and community engagement. Riverside Bridge School recognises that social media can be used positively to celebrate achievement, share information and promote the work of the school. However, inappropriate use may present safeguarding, reputational, professional and information security risks.

All members of the school community are expected to use social media responsibly and in a manner that reflects the values of Riverside Bridge School. Online communication and activity should demonstrate the same standards of respect, professionalism and courtesy that are expected in face-to-face interactions.

11.1 School accounts

Official school social media accounts will be managed only by authorised members of staff.

Content published through school accounts will:

- support the school's educational aims and values;
- protect the privacy and dignity of pupils and staff;
- comply with safeguarding and data protection requirements;
- reflect the school's professional standards;
- be accurate, respectful and appropriate for a public audience.

Appropriate oversight will be maintained to ensure that school accounts remain secure and that content is regularly monitored.

Before content is published through official school communication channels, staff responsible for approval should consider:

- Could this image or information identify an individual pupil?
- Is that identification necessary?
- Could the same message be communicated using a less identifiable image or description?
- Does publication remain appropriate when safeguarding, privacy and dignity are considered?

Where the answer to any of these questions raises concern, publication should be reconsidered or an alternative image or format should be used.

Where external organisations manage the school's website, photography, video production or social media on behalf of Riverside Bridge School, they must comply with the school's safeguarding, online safety, image consent and data protection requirements. Riverside Bridge School retains overall responsibility for approving content published in its name or on its behalf.

11.2 Staff use of social media

Staff are entitled to use personal social media outside work. However, they remain responsible for ensuring that their online conduct does not compromise their professional responsibilities or public confidence in the school.

Staff are expected to:

- maintain appropriate professional boundaries at all times;
- ensure that personal use of social media does not affect their professional role;
- use appropriate privacy settings on personal accounts;
- avoid publishing content that could undermine confidence in their professional judgement or the reputation of the school;
- report any safeguarding concerns encountered through social media in accordance with school procedures.
- Staff must not:
- communicate with pupils through personal social media accounts;
- accept or initiate personal social media connections with current pupils;
- share confidential or identifying information relating to pupils, families or colleagues;
- publish images or recordings obtained through their work unless authorised to do so;
- present personal opinions as representing the views of the school.

11.3 Pupils

Where appropriate to their age and stage of development, pupils will be supported to understand that social media should be used safely, respectfully and responsibly.

Learning may include:

- recognising appropriate and inappropriate online communication;
- understanding that information shared online may remain accessible;
- knowing how to seek help if something online causes concern;
- treating others with kindness and respect;
- understanding the importance of protecting personal information.

Teaching will always be adapted to meet individual communication and learning needs.

11.4 Parents and carers

The school values the positive relationships it has with parents and carers and recognises that social media is widely used to share information and celebrate children's achievements.

Parents and carers are encouraged to use social media responsibly and to consider the privacy, dignity and wellbeing of all members of the school community when sharing information or images relating to school activities.

Where concerns arise regarding the inappropriate use of social media which may affect pupils, staff or the wider school community, the school will seek to resolve these constructively and, where necessary, take appropriate action in accordance with its safeguarding and relevant school procedures.

11.5 Concerns arising from social media

Any social media activity that raises a safeguarding concern, places a child or adult at risk, constitutes harassment or bullying, involves unlawful activity or has the potential to damage the safe operation of the school will be taken seriously.

Such concerns will be managed in accordance with the Child Protection and Safeguarding Policy, Staff Code of Conduct, Positive Support Policy and relevant disciplinary procedures. Where appropriate, advice or support may also be sought from external agencies, including the Local Authority, police or other safeguarding partners.

Section 12

ONLINE RISKS AND SAFEGUARDING

Recognising risk. Identifying harm. Responding early.

Riverside Bridge School recognises that children and young people may experience a wide range of online risks. These risks continue to evolve as technology develops and may affect pupils in different ways depending upon their age, communication abilities, learning needs, level of independence and access to digital technology.

The school adopts a preventative, safeguarding-led approach to managing online risks. Staff are expected to remain professionally curious and recognise that online concerns rarely occur in isolation. In many cases, online incidents form part of wider safeguarding concerns and should be considered alongside information already known about the pupil.

The school categorises online risks using the recognised 4 Cs Framework.

12.1 Content risks

Content risks arise where a child is exposed to material that may be illegal, harmful, inappropriate or distressing.

This may include exposure to:

- violent or abusive material;
- pornography or sexually explicit content;
- hate speech or extremist material;
- self-harm or suicide-related content;
- misinformation or disinformation;
- harmful health or lifestyle advice;
- AI-generated or manipulated images, videos and audio intended to deceive.

The school seeks to reduce these risks through appropriate filtering, supervision, curriculum teaching and safeguarding intervention where concerns arise.

12.2 Contact risks

Contact risks occur where children are contacted by individuals who may seek to exploit, manipulate or harm them.

Examples include:

- online grooming;
- child sexual exploitation;

- child criminal exploitation;
- coercion or manipulation;
- radicalisation;
- financial scams or fraud;
- contact from strangers through games, messaging services or social media.

Staff remain vigilant to indicators that a pupil may be experiencing inappropriate online contact and will respond in accordance with safeguarding procedures.

12.3 Conduct risks

Conduct risks arise through a child's own online actions or interactions, or those of other people.

This may include:

- cyberbullying;
- online harassment;
- sharing inappropriate images or messages;
- image-based abuse;
- peer-on-peer abuse;
- misuse of artificial intelligence;
- creating or sharing harmful content;
- attempts to bypass school filtering or security systems.

The school recognises that pupils may not always understand the consequences of their online actions. Responses will therefore balance safeguarding, education and proportionate positive support whilst taking appropriate action where necessary.

12.4 Commercial risks

Commercial risks arise where children may be exploited for financial gain or encouraged to engage with inappropriate commercial activity.

Examples include:

- online scams;
- phishing;
- gambling;
- in-app purchases;
- misleading advertising;
- financial exploitation;
- theft of personal information.

Where appropriate, pupils will be taught strategies to recognise and avoid these risks as part of the wider curriculum.

12.5 Emerging risks

Technology continues to develop rapidly, and new online risks emerge regularly. Riverside Bridge School will keep its online safety arrangements under review and respond appropriately to emerging concerns identified through statutory guidance, safeguarding partners, professional advice or local intelligence.

This may include developments relating to artificial intelligence, immersive technologies, encrypted communication platforms, new social media applications or other digital services that may present safeguarding concerns.

12.6 Responding to online risks

Where an online concern is identified, the welfare of the child will always be the school's primary consideration.

Staff must report concerns without delay in accordance with the Child Protection and Safeguarding Policy.

Responses will be proportionate to the nature of the concern and may include safeguarding intervention, pastoral support, positive support, engagement with parents and carers, technical action, referral to external agencies or police involvement where appropriate.

The school recognises that effective safeguarding depends upon early identification, timely information sharing and collaborative working with families and partner agencies.

Section 13

MANAGING ONLINE SAFETY INCIDENTS

Responding promptly. Reporting concerns. Learning from incidents.

Despite appropriate education, supervision and technical safeguards, online safety incidents may still occur. Riverside Bridge School is committed to responding promptly, proportionately and consistently to all concerns involving the use of technology or online services.

Every concern will be considered in the context of the individual pupil's age, communication abilities, cognitive profile, additional needs and wider safeguarding circumstances. The welfare of the child will always remain the school's primary consideration.

Staff should not attempt to investigate safeguarding concerns independently beyond what is necessary to ensure immediate safety and preserve relevant information. Concerns should be reported promptly so that they can be managed through the school's safeguarding procedures.

13.1 Reporting concerns

All members of staff have a responsibility to report online safety concerns without delay.

Concerns may arise through:

- direct disclosure by a pupil;
- observations made by staff;
- filtering or monitoring alerts;
- reports from parents or carers;
- concerns raised by another pupil;
- information received from external agencies;
- inappropriate use of school technology.

Any concern that indicates a pupil may be at risk of harm must be reported immediately to the Designated Safeguarding Lead (DSL) or, in their absence, a Deputy Designated Safeguarding Lead.

13.2 Initial response

When responding to an online safety concern, staff should:

- ensure the immediate safety and wellbeing of the pupil;
- listen calmly and reassure the pupil where appropriate;
- avoid making promises of confidentiality;
- preserve relevant information or evidence where possible;
- not view, copy, download or forward suspected illegal imagery or content unnecessarily;

- seek immediate guidance from the DSL and follow safeguarding and police advice where applicable;
- report the concern immediately through the school's safeguarding procedures.

Where there is an immediate risk of significant harm, staff must take appropriate action to protect the pupil and seek urgent support from the DSL or emergency services where necessary.

13.3 Managing incidents

The Designated Safeguarding Lead will assess each concern in accordance with the Child Protection and Safeguarding Policy and determine the most appropriate course of action.

Depending on the nature of the incident, this may include:

- providing safeguarding or pastoral support;
- engaging with parents or carers;
- reviewing filtering or monitoring arrangements;
- implementing positive support or risk management measures;
- making referrals to Children's Social Care, the Police, CEOP or other relevant agencies;
- seeking advice from the Local Authority Designated Officer (LADO) where appropriate;
- reviewing individual support plans or risk assessments.

Where an incident involves potential criminal activity, the school will work with the police and other relevant agencies while ensuring that the welfare of the child remains central to decision-making.

13.4 Searching devices

There may be occasions where it is necessary to search, examine or retain a pupil's electronic device as part of managing a safeguarding concern.

Any such action will be carried out only where there is a lawful basis to do so and in accordance with current statutory guidance, including the Department for Education's guidance on Searching, Screening and Confiscation, the Child Protection and Safeguarding Policy and any relevant advice from safeguarding partners or the police.

The school will ensure that searches are proportionate, necessary and respectful of the rights, dignity and welfare of the pupil.

13.5 Recording and information sharing

Online safety concerns will be recorded using the school's safeguarding recording systems in the same way as any other safeguarding concern.

Information will be shared on a need-to-know basis and in accordance with safeguarding legislation, UK GDPR, the Data Protection Act 2018 and the school's Information Sharing procedures.

Accurate record keeping supports effective safeguarding, enables patterns of concern to be identified and assists the school in working collaboratively with families and partner agencies.

13.6 Learning from incidents

Where appropriate, the school will review significant online safety incidents to identify any lessons that can strengthen safeguarding practice.

This may include reviewing:

- curriculum provision;
- staff training;
- filtering and monitoring arrangements;
- supervision;
- individual risk assessments;
- communication with parents and carers;
- school procedures.

The purpose of these reviews is to promote continuous improvement and reduce the likelihood of similar incidents occurring in the future.

Section 14

REMOTE LEARNING, EDUCATIONAL VISITS AND OFF-SITE ACTIVITIES

Maintaining safeguards. Adapting arrangements. Protecting pupils.

Online safety expectations apply whenever pupils, staff or volunteers are using digital technology as part of school activities, regardless of location. The principles set out within this policy remain applicable during remote learning, educational visits, community activities and any other off-site provision organised by Riverside Bridge School.

The school recognises that different learning environments may present additional challenges. Appropriate planning, supervision and risk assessment will therefore be undertaken to ensure that technology continues to be used safely and appropriately.

14.1 Remote learning

Where remote learning or virtual communication is used, Riverside Bridge School will ensure that appropriate safeguarding arrangements remain in place.

This includes:

- using approved school platforms and communication systems;
- maintaining appropriate professional boundaries;
- protecting confidential information;
- ensuring online sessions are appropriate, secure and well supervised;
- following the school's safeguarding, data protection and acceptable use procedures.

Staff should ensure that any online learning activities are suitable for the individual needs of pupils and that reasonable adjustments are made where required.

14.2 Educational visits

Technology may be used during educational visits to support communication, learning, navigation, photography or emergency contact.

Where digital devices form part of an educational visit, staff will ensure that:

- their use supports the educational aims of the visit;
- pupils remain appropriately supervised;
- safeguarding and confidentiality are maintained;
- photographs and recordings are managed in accordance with school procedures;
- any online access is appropriate to the activity being undertaken.

Additional controls may be included within visit-specific risk assessments where technology presents an identified safeguarding or information security risk.

14.3 Off-site activities

Where pupils participate in off-site learning, work-related learning, community activities or alternative provision arranged by the school, online safety expectations remain unchanged.

The school will work with partner organisations, where appropriate, to ensure that safeguarding arrangements relating to technology are understood and that concerns are communicated promptly between agencies.

Section 15

MONITORING, REVIEW AND GOVERNANCE

Evaluating effectiveness. Identifying change. Strengthening practice.

Riverside Bridge School is committed to continually strengthening its online safety arrangements. The effectiveness of this policy will be monitored through safeguarding practice, staff feedback, curriculum review, technical assurance and governance oversight.

The school recognises that online safety is a rapidly evolving area. This policy will therefore be reviewed regularly to ensure that it continues to reflect current legislation, statutory guidance, technological developments and emerging safeguarding risks.

The Governing Board will receive appropriate assurance regarding the effectiveness of the school's online safety arrangements. This may include information relating to safeguarding trends, filtering and monitoring, cyber security, staff training, significant incidents and policy compliance.

The Headteacher and Designated Safeguarding Lead will ensure that lessons learned from incidents, audits and national guidance are reflected within school practice and staff development.

Section 16

RELATED POLICIES & FRAMEWORKS

Connecting practice. Strengthening consistency.

This policy should be read alongside the following school policies and procedures:

- Child Protection and Safeguarding Policy;
- Positive Support Policy;
- Mobile and Smart Technology Policy;
- Data Protection Policy;
- Staff Code of Conduct;
- Acceptable Use Agreements;
- Anti-Bullying Policy;
- Relationships, Sex and Health Education (RSHE) Policy;
- Educational Visits Policy;
- Information Security and Cyber Security procedures.

These documents collectively support the school's safeguarding framework and should be applied consistently where online safety concerns arise.

APPENDICES


RIVERSIDE BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE
ONLINE SAFETY
ROLES & REPORTING PATHWAY
Everyone has a part to play in keeping our school community safe online.
OUR ROLES
GOVERNING BOARD
Provides strategic oversight and assurance for online safety.
SENIOR LEADERSHIP TEAM
Promotes safe practice, monitors compliance and supports staff.
TECHNICAL SUPPORT PROVIDER
Manages filtering, monitoring, cyber security and provides technical advice.
HEADTEACHER
Overall responsibility for the implementation of this policy.
DESIGNATED SAFEGUARDING LEAD (DSL)
Leads all safeguarding concerns related to technology and online activity.
ALL STAFF
Supervise pupils, model safe use and report concerns immediately.
DEPUTY DSLs
Support the DSL and manage concerns in their absence.
PARENTS & CARERS
Work in partnership with the school to promote safe technology use.
PUPILS
Use technology safely and report concerns to a trusted adult.
REPORTING PATHWAY
1. Online concern identified
2. Report immediately to DSL / Deputy DSL
3. DSL assesses concern
4. Action taken & recorded
5. Review & follow-up
DSL RISK ASSESSMENT
LOW RISK
Education or pastoral support as required.
MEDIUM RISK
Support plan, monitoring and follow-up.
HIGH RISK
Immediate safeguarding action and possible external referral.
Parents / carers informed (where appropriate)
Referral to external agencies (if required)
Review, record and evaluate
Inspiring communication, empowering independence, achieving brighter futures.

RIVERSIDE
BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE

RESPONDING TO AN ONLINE SAFETY CONCERN

Our incident response flow

1. CONCERN IDENTIFIED
A concern is raised by a pupil, staff member, parent/carer or identified through monitoring.

2. IS ANYONE AT IMMEDIATE RISK?

YES
Ensure safety of pupil immediately.

NO
Preserve evidence where appropriate. Do not investigate alone.

3. REPORT TO DSL / DEPUTY DSL IMMEDIATELY

4. DSL RISK ASSESSMENT

LOW RISK
Education or pastoral support as required.

MEDIUM RISK
Support plan, monitoring and follow-up.

HIGH RISK
Immediate safeguarding action and possible external referral.

5. PARENTS / CARERS INFORMED
Where appropriate.

6. REFERRAL TO EXTERNAL AGENCIES
If required.

7. REVIEW, RECORD & EVALUATE

IMPORTANT REMINDERS

- Do not delete content. Preserve evidence.
- Do not investigate alone.
- Maintain professional curiosity and act without delay.
- Record all actions on Sleuth.
- The DSL will decide next steps and support required.

OUR PRINCIPLES

- Pupil safety is our priority.
- Respond quickly and appropriately.
- Record accurately and keep securely.
- Work in partnership with families.
- Learn and improve from every incident.

Inspiring communication, empowering independence, achieving brighter futures.

RIVERSIDE
BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE

FILTERING & MONITORING GOVERNANCE FRAMEWORK

Protecting our pupils online

AREA	WHO IS RESPONSIBLE	HOW OFTEN
Filtering Effectiveness	Technical Support Provider	Ongoing (24/7)
Monitoring Alerts	DSL / Authorised Safeguarding Staff	Daily / as alerts arise
Cyber Security	Technical Support Provider	Continuous
User Accounts & Access	School / Technical Provider	Ongoing
Software Updates	Technical Support Provider	Regular
Safeguarding Review	DSL	Ongoing
Governor Assurance	Headteacher / DSL	At least annually
Policy Review	SLT / Governors	Annual or sooner if required

OUR KEY PRINCIPLES

- Filtering supports safeguarding but does not replace supervision.
- Monitoring is proportionate and safeguarding-led.
- Alerts are reviewed promptly and acted on appropriately.
- Technical and safeguarding teams work collaboratively.
- Governors receive assurance rather than technical detail.

*Inspiring communication, empowering independence, achieving **brighter futures.***

*Inspiring communication, empowering independence, achieving **brighter futures.***

RIVERSIDE
BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE

EVERY MEMBER OF STAFF HAS A ROLE

Quick reference guide

SUPERVISE

Technology never replaces professional vigilance.

Be present, aware and proactive.

PROTECT

Keep pupils safe online through strong safeguarding practice and secure technology.

REPORT

Report any online concern immediately to the DSL / Deputy DSL. Never delay.

SECURE

Lock devices when unattended and protect passwords and information.

MODEL

Demonstrate positive digital behaviour in everything you do.

ESCALATE

If you are unsure, ask for advice. Safeguarding is everyone's responsibility.

Working together keeps our pupils safe, supported and able to thrive online.

KEY REMINDERS

- Use school systems and approved tools only.
- Listen to pupils and take online concerns seriously.
- Record concerns accurately on Sleuth.
- Work in partnership with families and the safeguarding team.
- Our shared actions create a safe online culture for all.

Inspiring communication, empowering independence, achieving brighter futures.

RIVERSIDE BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE

ONLINE SAFETY ACROSS THE CURRICULUM

Building knowledge, skills and confidence

Online safety is embedded throughout our curriculum to help pupils make safe, responsible choices and to prepare for life in a digital world.

FLOW 1A

Early Exploration

- Safe use of devices
- Recognising and expressing help
- Exploring cause and effect

FLOW 1B

Early Communication

- Online safety routines
- Communication safety
- Recognising safe adults
- Supported technology use

FLOW 2

Growing Independence

- Personal information
- Online friendships
- Respectful communication
- Recognising unsafe situations

FLOW 3

Preparing for Adulthood

- Social media
- Misinformation
- AI awareness
- Scams & online safety
- Online reputation
- Digital citizenship
- Preparation for Adulthood

THEMES REVISITED THROUGHOUT OUR CURRICULUM

Safe Use | Trusted Adults | Privacy | Respect | Communication | Digital Wellbeing | AI Awareness | Cyber Security | Preparation for Adulthood

HOW WE DELIVER THIS

- Age-appropriate teaching and experiences
- Real-life scenarios and practical activities
- Visual supports and accessible resources
- Opportunities to practise safe choices
- Links to personal development and wellbeing

We help pupils become confident, responsible digital citizens now and in the future.

PUPILS WILL BE ABLE TO

- Make safe choices online
- Recognise risks and seek help
- Communicate respectfully and responsibly
- Protect their personal information
- Use technology to learn, create and thrive

By learning about online safety in every pathway and every subject, we empower our pupils to achieve brighter futures.

Inspiring communication, empowering independence, achieving brighter futures.

RIVERSIDE
BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE

USING ARTIFICIAL INTELLIGENCE SAFELY

Protecting our pupils, our staff and our school

AI

Artificial Intelligence (AI) tools can support teaching, learning and administration. However, they must be used safely, responsibly and in line with our safeguarding duties and data protection obligations.

KEY RULES FOR STAFF

SAFEGUARDING FIRST

Pupil safety is our priority. Always consider the impact on pupils before using AI tools.

PROTECT INFORMATION

Do not enter, share or upload any personal, sensitive or confidential information about pupils, staff or families.

CHECK AND VERIFY

AI can make mistakes. Always check information, facts and sources before using or sharing.

USE PROFESSIONALLY

Use AI tools to support your role, not to replace professional judgement, creativity or relationships.

BE FAIR AND INCLUSIVE

Consider bias and fairness. Use AI tools in ways that are inclusive and do not discriminate.

FOLLOW SCHOOL POLICIES

Use AI tools in line with school policy, guidance and the law.

ALWAYS

- Use approved AI tools that have been recommended by the school.
- Read and understand the terms of use and privacy policy.
- Supervise and support pupils when AI tools are used in lessons.
- Report any concerns or misuse to the DSL.
- Keep a record of how AI tools are used and the impact on learning.

NEVER

- Enter, upload or share personal or sensitive information about anyone.
- Use AI tools that are not approved by the school.
- Rely on AI content without checking its accuracy or suitability.
- Download or copy AI-generated content without permission or a clear purpose.
- Share AI outputs that could identify or harm pupils, staff or our school.

Not sure? Ask your line manager or the DSL.
When in doubt, pause and check.

We use AI responsibly to enhance learning, not replace human connection.

Inspiring communication, empowering independence, achieving brighter futures.

RIVERSIDE
BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE

BEFORE YOU POST...

A Safeguarding Checklist

Sharing positive stories and celebrating our pupils' achievements is important.
Before you post or share an image, video or information online, pause and check.

☐ **Could this identify a pupil?**	Consider the pupil, their family or the location. Name, image, uniform, voice, or context may make them identifiable.
☐ **Is identification necessary?**	Do we need to identify the pupil or location to share the message? If not, leave it out.
☐ **Could a wider or less identifiable image be used?**	Use wider shots or group images where possible. Avoid close-ups or backgrounds that reveal identifying details.
☐ **Do I have the appropriate consent?**	Check we have the correct, up-to-date consent for the intended use and platform. If unsure, do not post.
☐ **Is publication in the child's best interests?**	Consider the potential impact on the pupil now and in the future. Would they be happy with this image being shared?
☐ **Could this image be copied or misused online or by AI?**	Once posted, content can be shared, downloaded or altered. Think about how it could be used beyond our control.

IF IN DOUBT, DON'T PUBLISH.
Seek advice before sharing.

Everyone has a responsibility to keep our pupils safe online. Thank you for helping to protect and promote their wellbeing.

Need advice?
Speak to the DSL or a member of SLT.

Inspiring communication, empowering independence, achieving brighter futures.