DATA PROTECTION POLICY

Protecting information. Respecting privacy.
Maintaining trust.



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 protecting personal information and meeting its responsibilities under UK data protection legislation. It establishes the principles, responsibilities and arrangements that govern how personal information is collected, used, recorded, stored, shared, retained and disposed of across the school.

Riverside Bridge School processes significant amounts of personal and sensitive information relating to pupils, families, staff and others who work with or support the school. This includes information relating to education, safeguarding, special educational needs and disabilities, health and medical needs, social care, communication, employment and the effective operation of the school. Protecting this information is fundamental to safeguarding individuals, respecting their rights and maintaining confidence in the school. As part of Partnership Learning Trust, Riverside Bridge School operates within the Trust's data-protection framework. Partnership Learning Trust is the Data Controller where it determines the purposes and means by which personal information is processed, supported by the Trust Data Protection Officer and the school's local data-protection arrangements.

The school will process personal information lawfully, fairly and transparently and in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 and other applicable legislation. Data protection will be considered throughout the lifecycle of information and incorporated into school systems, processes, decision-making and the introduction of new technologies.

Everyone who works for or on behalf of Riverside Bridge School has a responsibility to protect the personal information they access. Staff will be supported through appropriate systems, procedures, training and guidance and must seek advice where they are uncertain about the collection, use, sharing or security of personal information.

Our responsibilities to individuals

Riverside Bridge School will respect the information rights of pupils, parents and carers, staff and other individuals whose personal information we process. We will provide clear information about how personal data is used, maintain appropriate safeguards, respond appropriately to requests and concerns and take prompt action where information may have been lost, disclosed or otherwise compromised.

Particular care will be taken when processing information relating to children and young people and information that is sensitive because of its nature or the potential impact of inappropriate access, use or disclosure. Decisions about personal information will reflect both our legal responsibilities and our wider safeguarding responsibilities to pupils.

Through these commitments, Riverside Bridge School aims to ensure that personal information is handled lawfully, securely and respectfully throughout its lifecycle. We will continue to strengthen data-protection practice so that effective information governance supports safeguarding, professional practice, individual rights and the effective operation of the school.

RIVERSIDE BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE

TABLE OF CONTENTS

01	SCOPE	02	LEGISLATIVE FRAMEWORK
03	ROLES AND RESPONSIBILITIES	04	DATA PROTECTION OFFICER
05	DATA PROTECTION PRINCIPLES	06	LAWFUL PROCESSING OF PERSONAL DATA
07	PRIVACY INFORMATION	08	DATA ACCURACY AND QUALITY
09	DATA RETENTION AND DISPOSAL	10	INDIVIDUAL RIGHTS
11	INFORMATION SECURITY	12	DATA PROTECTION IMPACT ASSESSMENTS
13	SHARING PERSONAL INFORMATION	14	DATA PROCESSORS AND DIGITAL SERVICES
15	IMAGES, PHOTOGRAPHY AND VIDEO	16	CCTV
17	PERSONAL DATA BREACHES	18	TRAINING AND AWARENESS
19	MONITORING AND REVIEW		RELATED POLICIES AND FRAMEWORKS
	APPENDIX		

APPROVED BY: Governing Board

APPROVED ON: September 2026

REVIEWED DUE ON: September 2027

Section 01

SCOPE

Defining responsibilities. Establishing scope. Protecting personal information.

This policy applies to all personal data processed by Riverside Bridge School, whether information is held electronically, on paper, through audio or visual recordings, within an organised filing system or through any other medium used to process personal information.

It covers personal information relating to pupils and former pupils; parents, carers and family members; staff, former staff and job applicants; governors, trustees and volunteers; contractors, agency workers and professional partners; visitors and members of the public; and any other identifiable individual whose personal information is processed by or on behalf of the school.

The policy applies to all staff, governors, volunteers, agency workers, contractors and other individuals who process personal data on behalf of Riverside Bridge School or Partnership Learning Trust.

Partnership Learning Trust is the Data Controller where it determines the purposes and means of processing personal information across the Trust and its schools. Riverside Bridge School operates within the Trust's data-protection framework and works with the Trust Data Protection Officer in meeting these responsibilities.

This policy covers the complete lifecycle of personal information, from its collection and recording through to its use, sharing, storage, amendment, retention and eventual secure destruction.

All individuals working for or on behalf of the school must comply with this policy and the procedures and controls that support it. Failure to do so may result in disciplinary, contractual, regulatory or legal action as appropriate.

Section 02

LEGISLATIVE FRAMEWORK

Meeting legal duties. Maintaining accountability. Responding to change.

Riverside Bridge School will manage personal information in accordance with the legal and regulatory framework applying to the school and Partnership Learning Trust.

The principal legislation and guidance informing this policy includes:

- the UK General Data Protection Regulation;
- the Data Protection Act 2018;
- the Data (Use and Access) Act 2025;
- the Privacy and Electronic Communications Regulations;
- the Freedom of Information Act 2000, where applicable;
- the Human Rights Act 1998;
- relevant education, safeguarding and employment legislation; and
- guidance issued by the Information Commissioner's Office and Department for Education.

The Data (Use and Access) Act 2025 amended aspects of the UK data-protection framework rather than replacing the UK GDPR or Data Protection Act 2018. The school and Trust will keep their arrangements under review as provisions of the Act and associated regulatory guidance are implemented.

Data protection requires more than compliance with individual rules. The school and Trust must also be able to demonstrate accountability through appropriate policies, privacy information, records of processing, contracts, retention arrangements, risk assessments, training, security measures and records of significant decisions.

This policy should therefore be read as part of the wider Riverside Bridge School and Partnership Learning information-governance framework.

Section 03

ROLES AND RESPONSIBILITIES

Clarifying accountability. Sharing responsibility. Maintaining oversight.

Effective data protection is a shared responsibility. Everyone who accesses, records, uses or shares personal information must understand their responsibilities and handle information appropriately.

As Data Controller where it determines the purposes and means of processing, **Partnership Learning Trust has overall responsibility for the Trust-wide data-protection** framework.
The Trust is responsible for maintaining appropriate governance arrangements, appointing a suitably qualified Data Protection Officer, establishing appropriate policies and procedures, ensuring suitable technical and organisational safeguards are in place and overseeing contractual arrangements with organisations processing personal information on its behalf.
The Trust will support its schools in meeting their data-protection responsibilities and provide appropriate assurance to trustees and governing boards.

The Governing Board provides local strategic oversight and assurance. It will monitor the school's implementation of this policy, seek assurance that significant data-protection and information-security risks are being managed and ensure that appropriate arrangements support compliance.
Governors must maintain confidentiality when handling personal information and must not access or use information obtained through their governance role for unrelated or personal purposes. Governors will complete data-protection training appropriate to their responsibilities.

The Headteacher has overall responsibility for ensuring that this policy is implemented effectively within Riverside Bridge School.
The Headteacher will promote a culture in which privacy and information security are taken seriously, ensure that staff understand their responsibilities, support effective local data-protection arrangements and ensure that significant concerns or breaches are escalated appropriately.

Data protection will be considered as part of school decision-making, particularly where new systems, technologies, services or significant information-processing arrangements are proposed.

Riverside Bridge School will designate a **School Data Protection Lead** to coordinate day-to-day data-protection arrangements and act as the principal school contact for information-governance matters.

The School Data Protection Lead will liaise with the Trust Data Protection Officer; support the maintenance of appropriate information-governance records; coordinate information-rights requests and local breach responses; support privacy notices, retention arrangements and Data Protection Impact Assessments; provide guidance to staff; and promote appropriate training and awareness.

The designation of the School Data Protection Lead may change without requiring amendment of this policy, provided that responsibility is formally allocated and communicated.

All staff, governors, volunteers and authorised users handling personal information must access only information required for their role and use it only for authorised purposes. They must follow approved security arrangements, maintain confidentiality, keep records appropriately accurate, protect authentication information and take reasonable care when sending, sharing, storing or disposing of personal information.

Actual or suspected data breaches, security incidents or inappropriate access must be reported immediately through the school's established reporting arrangements.

Where an individual is uncertain about how personal information may lawfully or safely be used, shared, stored or disposed of, they must seek advice before acting.

Section 04

DATA PROTECTION OFFICER

Providing independent advice. Monitoring compliance. Supporting accountability.

Partnership Learning Trust will appoint a Data Protection Officer in accordance with applicable data-protection legislation.

The Data Protection Officer operates independently and provides specialist advice, oversight and challenge in relation to the Trust's and schools' data-protection responsibilities.

The Data Protection Officer's functions include advising the Trust and its schools about their legal obligations, monitoring compliance, supporting training and awareness, advising on Data Protection Impact Assessments, supporting the management of personal data breaches and information-rights requests and liaising with the Information Commissioner's Office where required.

The Data Protection Officer will also provide advice where proposed processing presents significant or complex privacy risks or where the appropriate interpretation of data-protection requirements is uncertain.

Questions that cannot be resolved through the school's local arrangements will be referred to the Trust Data Protection Officer through the School Data Protection Lead where appropriate.

Current contact details for the Data Protection Officer will be published through relevant privacy notices and other appropriate channels rather than being fixed within this policy.

Section 05

DATA PROTECTION PRINCIPLES

Processing fairly. Limiting information. Demonstrating accountability.

The UK GDPR establishes principles that apply whenever personal information is processed. These principles underpin Riverside Bridge School's information-governance arrangements and apply throughout the lifecycle of information.

Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- retained for no longer than necessary;
- protected through appropriate technical and organisational measures; and
- managed in a way that enables the Data Controller to demonstrate compliance with these principles.

These principles will be considered whenever the school designs a process, collects information, makes decisions about its use or sharing, introduces a new system or service, retains information or determines that information should be destroyed.

Data protection by design and by default will form part of school planning and decision-making rather than being considered only after processing has begun.

Section 06

LAWFUL PROCESSING OF PERSONAL DATA

Identifying purpose. Establishing lawful basis. Protecting sensitive information.

Riverside Bridge School will only process personal information where there is a clear purpose and an appropriate lawful basis. Depending on the purpose and circumstances, processing may be necessary because of a legal obligation, the performance of a public task or exercise of official authority, the performance of a contract, protection of vital interests, legitimate interests where this basis is available and appropriate, recognised legitimate interests where the statutory requirements are met, or valid consent. For much of the school's core educational, safeguarding and statutory work, consent will not be the appropriate lawful basis. The school will not seek consent where another lawful basis more accurately reflects the nature of the processing or where individuals do not have a genuine choice about whether the processing occurs.

Where consent is relied upon, it will be freely given, specific, informed and unambiguous and capable of being withdrawn. The school will maintain appropriate evidence of consent and make withdrawal reasonably straightforward.

The lawful basis for processing will be identified before processing begins and reflected appropriately within privacy information and records of processing.

Special category and criminal offence information

Riverside Bridge School routinely processes information requiring enhanced protection, including information relating to health, disability and other special category data.

Where special category personal data is processed, the school and Trust will identify both an appropriate Article 6 lawful basis and an applicable Article 9 condition. Where required, the relevant condition under the Data Protection Act 2018 will also be identified.

Criminal offence data will only be processed where the legal requirements for doing so are met and appropriate safeguards are maintained. Particular care will be taken when sensitive information relates to pupils because inappropriate access, loss or disclosure may create safeguarding or other significant risks. Where the lawful basis or additional processing condition is uncertain, advice will be sought from the School Data Protection Lead or Trust Data Protection Officer before processing proceeds.

Section 07

PRIVACY INFORMATION

Explaining clearly. Processing transparently. Maintaining trust.

Riverside Bridge School will be open and transparent about how personal information is collected, used, shared and retained.

Appropriate privacy information will explain the types of personal information collected, why it is required, the lawful basis for processing, who information may be shared with, relevant retention arrangements, the rights available to individuals and how questions or concerns can be raised.

Privacy notices will be made available to pupils, parents and carers, staff, applicants, volunteers and other individuals as appropriate.

Information will be written and presented in a way that is clear and accessible to the intended audience. Where information is provided directly to pupils, consideration will be given to their age, communication needs and level of understanding.

Privacy information will be reviewed periodically and when significant changes are made to the purpose or nature of processing.

Where personal information is to be used for a materially different purpose, the school will consider whether updated privacy information, a revised lawful basis or other action is required before that processing begins.

Section 08

DATA ACCURACY AND QUALITY

Maintaining accuracy. Correcting promptly. Supporting sound decisions.

Riverside Bridge School will take reasonable steps to ensure that personal information is accurate, complete and, where necessary, kept up to date.

The importance of accuracy will be proportionate to the purpose for which information is being used. Particular care will be taken where inaccurate information could affect safeguarding, health and medical support, SEND provision, educational decisions, family communication, employment or an individual's rights.

The school will maintain appropriate arrangements for updating key records and will encourage pupils, families, staff and others to inform the school when relevant information changes.

Where inaccurate or incomplete information is identified, reasonable steps will be taken to correct it without undue delay and, where appropriate, to ensure that connected systems or recipients are also updated.

Where an individual challenges the accuracy of information held about them, the matter will be considered in accordance with data-protection legislation and the school's information-rights arrangements.

Section 09

DATA RETENTION AND DISPOSAL

Keeping proportionately. Reviewing regularly. Disposing securely.

Personal information will be retained only for as long as it is necessary for the purpose for which it is held or to meet statutory, safeguarding, contractual, regulatory or legitimate operational requirements.

Detailed retention periods will be established through the school and Trust's approved retention arrangements and the Riverside Bridge School Data Retention Schedule.

Retention decisions will take account of applicable legislation, Department for Education guidance, safeguarding requirements, Trust arrangements and recognised records-management practice.

Records must not be retained indefinitely merely because they may be useful in the future. Equally, information must not be destroyed where it remains subject to a safeguarding, legal, regulatory, information-access or other legitimate hold.

When records reach the end of their applicable retention period and no continuing justification exists, they will be securely destroyed or appropriately anonymised.

Paper and electronic records will be disposed of using methods appropriate to their sensitivity and format so that confidential or personal information cannot reasonably be reconstructed or accessed by unauthorised individuals.

Detailed requirements are set out within the school's Data Retention Policy and Data Retention Schedule.

Section 10

INDIVIDUAL RIGHTS

Respecting rights. Responding appropriately. Providing effective routes for challenge.

Riverside Bridge School recognises and will support the rights individuals have in relation to their personal information.

Depending on the circumstances and lawful basis for processing, these may include rights to be informed about processing, access personal information, correct inaccurate information, request erasure or restriction, object to processing, receive information in a portable format where applicable and receive appropriate safeguards in relation to automated decision-making.

Not every right applies to every processing activity. Some rights are subject to statutory conditions, restrictions or exemptions, particularly where information relates to safeguarding, third parties, legal obligations or the exercise of official authority.

Requests will be recognised and managed promptly and in accordance with applicable statutory requirements. Subject Access Requests will be managed in accordance with the school's separate Subject Access Request Policy.

Where a request cannot be fulfilled in whole or in part, the individual will be given an appropriate explanation and information about any available route for review or complaint.

Data-protection complaints

Individuals may raise concerns or complaints about the school's handling of their personal information. Complaints will be acknowledged and considered through the school and Trust's established data-protection arrangements. The school will cooperate with the Trust Data Protection Officer in investigating concerns and providing an appropriate response. Individuals will also be informed of their right to raise a concern with the Information Commissioner's Office where applicable.

Section 11

INFORMATION SECURITY

Protecting information. Controlling access. Maintaining confidentiality.

Riverside Bridge School will maintain appropriate technical and organisational measures to protect personal information against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

Security arrangements will be proportionate to the sensitivity of the information, the risks associated with its processing and the potential consequences for individuals if information is compromised.

Access to personal information will be limited to individuals who require it for legitimate purposes. Approved systems, appropriate authentication, access controls, secure storage, backup arrangements and physical safeguards will be used as appropriate.

Staff must follow the school and Trust's requirements for secure working, including when accessing information remotely or using mobile devices.

Detailed information-security requirements are established through the Information Security Policy, ICT Acceptable Use Policy, associated Trust ICT arrangements and relevant operational procedures.

Actual or suspected security incidents must be reported immediately.

Section 12

DATA PROTECTION IMPACT ASSESSMENTS

Identifying risk. Designing safely. Protecting privacy from the outset.

Riverside Bridge School is committed to data protection by design and by default.

A Data Protection Impact Assessment (DPIA) will be completed where proposed processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA may also be used where it provides a proportionate means of understanding and reducing significant privacy risks even where the statutory threshold is uncertain.

Particular consideration will be given where proposed processing involves new technologies; new EdTech or digital platforms processing pupil information; AI or automated processing; systematic monitoring; large-scale processing of special category information; significant new information-sharing arrangements; or processing involving children or other individuals who may be particularly vulnerable.

The need for a DPIA should be considered before a new system, technology or significant processing activity is introduced.

The School Data Protection Lead will work with relevant staff and the Trust Data Protection Officer to identify the purpose of the processing, assess necessity and proportionality, identify risks to individuals and determine appropriate safeguards.

Where a DPIA identifies high residual risk that cannot be adequately mitigated, processing will not commence until appropriate advice has been obtained and any further statutory requirements have been met.

DPIAs will be reviewed where significant changes occur to the nature, purpose, technology or risks associated with the processing.

Section 13

SHARING PERSONAL INFORMATION

Sharing lawfully. Protecting confidentiality. Supporting effective partnership.

Riverside Bridge School works with a wide range of organisations and professionals and recognises that appropriate information sharing is essential to education, safeguarding, health, SEND provision and effective partnership working.

Personal information will only be shared where there is a lawful basis for doing so and the information shared is relevant, necessary and proportionate to the purpose.

Recipients may include the Department for Education, local authorities, health and social care professionals, safeguarding partners, other educational settings, examination and awarding organisations, contracted service providers and other organisations where sharing is required or permitted by law.

Before sharing personal information, staff must consider the purpose of the sharing, whether there is an appropriate lawful basis, what information is genuinely required, who needs to receive it and how it can be shared securely.

Information sharing does not always require consent. In particular, safeguarding information may and should be shared without consent where there is a lawful basis and sharing is necessary to protect a child or another individual.

Concerns about data protection must not be used as a reason to withhold information where sharing is necessary and lawful to safeguard a pupil. Equally, safeguarding must not be used as a justification for indiscriminate or disproportionate disclosure.

Where there is uncertainty, advice should be sought from the DSL, School Data Protection Lead or Trust Data Protection Officer as appropriate.

Section 14

DATA PROCESSORS AND DIGITAL SERVICES

Selecting carefully. Contracting appropriately. Maintaining oversight.

Partnership Learning Trust and Riverside Bridge School use external organisations and digital services that process personal information on their behalf.

These may include management information systems, educational and assessment platforms, communication systems, payment and catering systems, payroll services, ICT support, cloud services and other specialist educational technologies.

Where an organisation processes personal information on behalf of the Data Controller, appropriate due diligence will be undertaken before the service is approved. This will include consideration of data protection, information security, processing locations, sub-processors, retention and deletion arrangements and the provider's ability to meet applicable legal requirements.

Appropriate contractual terms will be established in accordance with UK data-protection legislation.

New EdTech, cloud-based services, applications or AI-enabled systems must not be introduced for processing school personal information solely because they are readily available or educationally useful. Appropriate school or Trust approval must be obtained and data-protection and information-security implications considered before use.

Where the proposed processing is likely to create high risk, a Data Protection Impact Assessment will be completed.

The Trust and school will maintain appropriate oversight of processing arrangements and will take action where a provider no longer meets required standards.

Section 15

IMAGES, PHOTOGRAPHY AND VIDEO

Using images responsibly. Respecting choices. Protecting pupils.

Riverside Bridge School recognises the value of photographs and video in supporting learning, recording progress, celebrating achievement and communicating school life while also recognising the privacy and safeguarding implications of their use.

Images and recordings may be processed for educational, assessment, safeguarding, operational or promotional purposes where there is an appropriate lawful basis.

Where consent is the appropriate basis, the school will maintain suitable consent arrangements and respect withdrawal of consent in relation to future use where applicable. Where another lawful basis applies, the school will ensure that the processing remains necessary, proportionate and transparent.

Images will be stored and shared only through approved arrangements and will not be used for purposes incompatible with those for which they were obtained.

Particular consideration will be given to safeguarding restrictions, pupil vulnerability and the wishes and rights of the individual concerned. As pupils develop greater understanding and capacity, their views will be given appropriate weight alongside parental or carer involvement.

Parents and carers attending school events may take photographs or recordings for personal and domestic purposes unless the school advises otherwise. They will be expected to respect the privacy and safeguarding needs of other pupils and adults and not publish identifiable images of others without appropriate permission.

Staff must follow the school's specific arrangements governing photography, recording and use of personal devices.

Section 16

CCTV

Monitoring proportionately. Protecting safety. Respecting privacy.

Riverside Bridge School operates Closed-Circuit Television systems to support the safety and security of pupils, staff, visitors, premises and school assets.

CCTV will only be used for defined and legitimate purposes and its operation will be lawful, necessary, proportionate and transparent.

Appropriate signage and privacy information will be provided. Access to recordings will be restricted and recordings will be retained and disclosed only in accordance with the approved arrangements.

The detailed operation, management, retention, access and disclosure of CCTV recordings is governed by the CCTV Policy and associated procedures.

Any introduction or significant alteration of surveillance arrangements will be considered from a data-protection-by-design perspective and a DPIA completed where required.

Section 17

PERSONAL DATA BREACHES

Recognising quickly. Reporting immediately. Protecting people.

Riverside Bridge School takes all actual and suspected personal data breaches seriously.

A personal data breach may involve the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal information. Breaches may affect the confidentiality, integrity or availability of information.

All staff, governors, volunteers, contractors and other authorised users must report an actual or suspected breach immediately through the school's established reporting arrangements. Staff must report concerns even where they are uncertain whether an incident meets the legal definition of a personal data breach.

The school will take proportionate immediate action to contain incidents and will notify the Trust Data Protection Officer without undue delay so that the nature, scale and potential impact of the breach can be assessed.

Where statutory thresholds are met, Partnership Learning will coordinate notification to the Information Commissioner's Office and, where required, affected individuals.

All confirmed breaches will be appropriately documented and reviewed so that lessons can be identified and information-governance arrangements strengthened.

Detailed reporting, assessment, notification and review arrangements are set out in the Data Breach Response Policy.

Section 18

TRAINING AND AWARENESS

Building understanding. Strengthening practice. Maintaining responsibility.

Effective data protection depends on individuals understanding their responsibilities and applying them consistently.

Staff will receive appropriate data-protection and information-security training as part of induction and refresher training will be provided periodically. Governors, volunteers and others who process personal information will receive training or guidance proportionate to their roles.

Training and awareness will address the principles of data protection, confidentiality, information security, safe information sharing, records management, recognising and reporting breaches, cyber-security risks and relevant changes to legislation or school and Trust arrangements.

Additional or targeted training will be provided where monitoring, incidents, changes in systems or identified risks demonstrate a particular need.

Staff are expected to apply their training in practice and seek advice whenever they are uncertain about the appropriate handling of personal information.

Section19

MONITORING AND REVIEW

Monitoring compliance. Maintaining oversight. Strengthening practice.

The Headteacher has overall responsibility for ensuring that effective data-protection arrangements are maintained within Riverside Bridge School. The School Data Protection Lead will coordinate day-to-day monitoring and work with the Trust Data Protection Officer and relevant school and Trust colleagues to promote effective information governance.

Monitoring will consider compliance with data-protection requirements, information-rights requests, personal data breaches, information-security incidents, retention arrangements, DPIAs, privacy information, staff training and emerging risks associated with systems or working practices. Patterns or recurring concerns will be used to identify where changes to procedures, systems, training or organisational controls are required.

Significant compliance concerns, high-risk processing issues or serious incidents will be escalated appropriately to the Headteacher, Trust Data Protection Officer and Partnership Learning.

The Governing Board will receive appropriate assurance that data-protection responsibilities are being met, significant risks are being managed, appropriate information-security arrangements are in place and staff receive suitable training and support.

This policy will be reviewed annually, or sooner where changes to legislation, regulatory guidance, Trust arrangements, technology or school operations require amendment. Operational procedures, privacy information and guidance may be updated between formal policy reviews where necessary, provided that they remain consistent with this policy and applicable Trust requirements.

Section 20

RELATED POLICIES & FRAMEWORKS

Connecting practice. Strengthening consistency.

This policy forms part of Riverside Bridge School's wider information-governance arrangements and should be read alongside:

- Privacy Notices
- Subject Access Request Policy
- Data Retention Policy
- Freedom of Information Policy
- Information Security Policy
- Data Breach Response Policy
- ICT Acceptable Use Policy
- Online Safety Policy
- CCTV Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Risk Management and Risk Assessment Policy
- Partnership Learning information-governance and ICT security arrangements

Detailed operational guidance, registers, forms, privacy notices, DPIAs, information-sharing arrangements, data-breach records and other working documents will be maintained separately from this policy.

They may be updated as legislation, regulatory guidance, Trust requirements, technology or operational arrangements change without requiring formal revision of this policy, provided that they remain consistent with its principles and requirements.

APPENDIX

RIVERSIDE BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE

DATA PROTECTION
EVERYONE'S RESPONSIBILITY

Protecting information. Respecting privacy. Maintaining trust.

THE INFORMATION LIFECYCLE

Think about data protection at every stage. Only collect, use, share, store and dispose of personal information when it is necessary, lawful and secure.

1 COLLECT — Only what is needed

- Collect personal information only for a clear, lawful purpose.
- Only collect what is relevant and necessary.
- Be transparent about why the information is needed.

BE PURPOSEFUL

2 USE — Only as authorised

- Use personal information only for authorised purposes.
- Only use as much information as is necessary.
- Keep information accurate and up to date.

USE RESPONSIBLY

3 SHARE — Only where lawful

- Share personal information only where there is a lawful basis.
- Only share with those who need it for a legitimate purpose.
- Check that information is sent securely and to the correct recipient.

SHARE SAFELY

4 STORE — Keep it secure

- Keep personal information secure and protect it from unauthorised access, loss or disclosure.
- Use approved systems and secure storage.
- Follow school and Trust guidance on accessing information remotely or on mobile devices.

KEEP IT SECURE

5 DISPOSE — When no longer needed

- Dispose of information securely when it is no longer required.
- Follow the school's Data Retention Schedule and approved disposal methods.
- Ensure information cannot be reconstructed or accessed by unauthorised individuals.

DISPOSE SECURELY

EVERYDAY EXPECTATIONS FOR ALL STAFF

- **Lock your screen** when you step away from your device.
- **Protect your passwords** and keep login details confidential.
- **Report lost or stolen devices** immediately.
- **Check recipients** before sending emails and attachments.
- **Use approved systems** and school/Trust platforms only.
- **Report concerns** including suspected data breaches, without delay.
- **Collect printing** immediately and keep documents secure.
- **Dispose of information** securely (e.g. shredding paper, secure deletion electronically).
- **Seek advice** from the School Data Protection Lead if you are uncertain.

STOP • THINK • PROTECT

If you are unsure whether personal information can be used, shared, stored or disposed of, seek advice from the School Data Protection Lead before taking action.

Inspiring communication, empowering independence, achieving brighter futures.