# DATA BREACH RESPONSE POLICY

**Recognising quickly. Reporting immediately.**
**Protecting people.**



## 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 recognising, reporting, managing and learning from personal data breaches. It establishes the responsibilities and arrangements through which the school responds promptly to actual or suspected breaches, limits potential harm and complies with its data-protection obligations.

Riverside Bridge School is committed to protecting the personal information entrusted to us by pupils, families, staff, governors, volunteers and others who interact with the school. Appropriate technical, physical and organisational safeguards are maintained to reduce the likelihood of information being lost, disclosed, altered, destroyed or accessed without authority. Despite these safeguards, personal data breaches can occur through human error, technical failure, cyber-attack, inappropriate disclosure, loss or other incidents. Prompt reporting is critical. Early action enables the school and Partnership Learning to contain an incident, assess the potential impact on individuals and determine whether statutory notification or other protective action is required.

As part of Partnership Learning, Riverside Bridge School works with the Trust Data Protection Officer to investigate and manage personal data breaches in accordance with the UK GDPR, Data Protection Act 2018, the Data (Use and Access) Act 2025 and relevant regulatory guidance. The school will maintain clear arrangements so that all staff understand how to recognise a potential breach and where to report concerns immediately. Current DfE guidance, updated in July 2026, continues to emphasise that all school staff have responsibility for protecting personal information and knowing what to do when something goes wrong.

The school promotes an open reporting culture. Staff are expected to report errors and concerns immediately and should not delay because they are uncertain whether an incident constitutes a breach or because they are concerned that they may have made a mistake. Honest mistakes reported promptly will be managed proportionately; deliberate misuse of information or knowingly failing to report a breach may be addressed through the school's disciplinary arrangements.

**Our responsibilities to individuals**

Riverside Bridge School will act promptly to protect individuals where their personal information may have been compromised. We will contain and investigate reported incidents, assess the likelihood and severity of potential harm, maintain appropriate records and work with the Trust Data Protection Officer to determine whether notification to the Information Commissioner's Office, affected individuals or another organisation is required.

We will communicate appropriately and transparently where individuals need to be informed and will use learning from breaches, near misses and recurring patterns to strengthen information security, staff practice and organisational controls.

Through these commitments, Riverside Bridge School aims to ensure that personal data breaches are recognised quickly, reported without delay and managed consistently and proportionately. We will continue to strengthen our information-governance arrangements so that the rights, privacy and safety of individuals remain central to our response.

RIVERSIDE BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE

# TABLE OF CONTENTS


| | | | |
|---|---|---|---|
| 01 | PURPOSE AND SCOPE | 02 | WHAT IS A PERSONAL DATA BREACH? |
| 03 | ROLES AND RESPONSIBILITIES | 04 | REPORTING A SUSPECTED DATA BREACH |
| 05 | MANAGING AND ASSESSING A DATA BREACH | 06 | NOTIFICATION AND COMMUNICATION |
| 07 | LEARNING FROM DATA BREACHES | 08 | TRAINING AND AWARENESS |
| 09 | MONITORING AND REVIEW | 10 | RELATED POLICIES AND FRAMEWORKS |
| | APPENDIX | | |


**APPROVED BY:** Governing Board

**APPROVED ON:** September 2026

**REVIEWED DUE ON:** September 2027

Section 01

# PURPOSE AND SCOPE

Defining responsibilities. Establishing scope. Supporting rapid response.

The purpose of this policy is to ensure that Riverside Bridge School responds promptly, consistently and effectively to actual or suspected personal data breaches.

It establishes the school's arrangements for recognising potential breaches, reporting concerns without delay, containing incidents, assessing risk, working with Partnership Learning and the Trust Data Protection Officer, meeting statutory notification requirements and learning from incidents.

Prompt action can significantly reduce the impact of a breach. The school therefore expects concerns to be reported at the earliest opportunity, even where the individual reporting the matter is unsure whether a personal data breach has occurred.

This policy applies to all staff, governors, volunteers, agency staff, contractors and other persons who process personal information on behalf of Riverside Bridge School.

It applies to personal information in any format, including electronic records, paper documents, photographs, audio and video recordings, emails, cloud systems, management information systems, portable devices and any other medium through which personal information is processed.

The policy covers information relating to pupils, parents and carers, staff, governors, volunteers, applicants, visitors, contractors and any other identifiable individual whose personal information is processed by the school.

It applies to suspected and confirmed personal data breaches arising accidentally or deliberately, including incidents caused by human error, system failure, cyber-security threats, unauthorised disclosure or inappropriate access.

This policy should be read alongside the Partnership Learning Data Breach Notification Policy and the school's wider Data Protection and Information Security arrangements.

Section 02

# WHAT IS A PERSONAL DATA BREACH?

Recognising incidents. Understanding risk. Reporting uncertainty.

A personal data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

A breach may affect the confidentiality, integrity or availability of information. It therefore includes more than simply losing data.

Examples may include:

- emailing confidential information to the wrong recipient;
- sending an EHCP, report or other pupil record to the wrong family;
- losing paper records containing personal information;
- leaving confidential documents in an unsecured location;
- misplacing a communication book or other pupil record containing sensitive information;
- losing a laptop, tablet, mobile phone or removable storage device containing or providing access to school information;
- sharing medical, safeguarding or other sensitive information with an unauthorised person;
- uploading information to the wrong Teams channel, shared folder or online platform;
- accidentally deleting or altering important personal information;
- losing access to personal information because of ransomware or another system incident;
- leaving printed reports on a printer or photocopier;
- unauthorised access to school accounts or systems.

Not every security incident will ultimately meet the definition of a personal data breach, and not every personal data breach will require notification to the ICO. However, every suspected breach must be reported immediately so that an appropriate assessment can be carried out.

Where there is doubt, staff must report the concern rather than attempt to determine the legal position themselves.

Section 03

# ROLES AND RESPONSIBILITIES

Clarifying accountability. Coordinating response. Protecting individuals.

Protecting personal information and reporting potential breaches is the responsibility of everyone working on behalf of Riverside Bridge School. Specific responsibilities are allocated to ensure that incidents can be escalated, assessed and managed effectively.

**The Governing Board** will receive appropriate assurance that effective data-breach arrangements are in place and that significant information-governance risks are being addressed. The Board will support an organisational culture of accountability, openness and continuous improvement.

**The Headteacher** has overall responsibility for ensuring that this policy is implemented effectively. The Headteacher will ensure that suspected breaches are taken seriously, appropriate immediate action is supported, the Trust Data Protection Officer is engaged through the agreed reporting route and lessons arising from significant incidents are acted upon.

**The School Data Protection Lead** coordinates the school's local response to suspected personal data breaches. The School Data Protection Lead will:

- receive and record reports of suspected breaches;
- support appropriate immediate containment;
- gather relevant information about the incident;
- liaise promptly with the Trust Data Protection Officer;
- coordinate local investigation where required;
- maintain appropriate breach records;
- support staff involved in the response;
- monitor incidents and trends to identify improvements.

**The Trust Data Protection Officer** provides specialist advice and oversight in accordance with Trust arrangements. The DPO will advise on the assessment of risk, determine whether statutory notification requirements are met, support communication with affected individuals, advise on external notifications and support investigation and learning.

**ICT Support** will support the containment, investigation and recovery of incidents involving digital systems, accounts, devices or cyber-security threats. Technical action will be coordinated with the School Data Protection Lead and Trust DPO as appropriate.

**All staff and other authorised users** must protect personal information, report suspected breaches immediately, cooperate with investigations, preserve relevant evidence, maintain confidentiality and follow instructions issued as part of the breach response.
Failure to report a known breach may itself constitute a breach of this policy.

Section 04

# REPORTING A SUSPECTED DATA BREACH

Reporting immediately. Preserving evidence. Limiting harm.

Every actual or suspected personal data breach must be reported immediately.

Staff must not delay reporting because they are uncertain whether a breach has occurred, believe somebody else may have reported it, are trying to resolve the issue themselves or are concerned that they may have made a mistake.

Where it is safe and appropriate to do so, the person identifying the incident should take reasonable immediate action to prevent further disclosure or loss. This may include recalling an email, securing a paper document, closing access to information or preserving relevant evidence.

However, staff must not undertake their own investigation or take technical action that could compromise evidence, interfere with system recovery or increase the impact of the incident.

The incident must be reported promptly to the School Data Protection Lead. If that person is unavailable, it must be escalated immediately to the Headteacher or through the Trust's agreed Data Protection Officer reporting route.

The initial report should include, where known:

- what happened;
- when it happened or was discovered;
- what information may be affected;
- who may be affected;
- how the incident occurred;
- whether the information has been recovered or remains accessible to an unauthorised person;
- what immediate action has already been taken.

Staff must not contact the ICO, media or affected individuals about the breach unless specifically authorised through the agreed response arrangements.

Section 05

# MANAGING AND ASSESSING A DATA BREACH

Containing incidents. Assessing risk. Recording decisions.

Once a suspected breach has been reported, Riverside Bridge School will act promptly to contain the incident, gather relevant information and assess the potential consequences.

**Containment**

Containment action will depend on the nature of the breach. Measures may include recalling emails, contacting unintended recipients and requesting secure deletion, recovering paper records, securing affected areas, restricting access to systems, disabling compromised accounts, remotely securing devices or involving ICT Support.

Containment should prioritise reducing continuing risk while preserving information required for investigation.

**Assessment**

The School Data Protection Lead and Trust Data Protection Officer will assess the circumstances of the incident, including the nature and sensitivity of the information affected, the number and vulnerability of people involved, whether safeguarding or special-category information is involved, whether information was encrypted or otherwise protected, who may have accessed the information and the potential consequences for affected individuals.

The assessment will focus primarily on the risk to the rights and freedoms of individuals. This includes the likelihood and severity of potential physical, financial, emotional, social, safeguarding or other harm. ICO guidance makes clear that the risk assessment must consider both the seriousness of the possible consequences and how likely they are to occur.

**Recording**

Every confirmed personal data breach will be documented, whether or not it reaches the threshold for notification to the ICO.

The record will include the facts of the breach, its effects or potential effects, the risk assessment undertaken, remedial action taken, notifications made or considered and the reasons for significant decisions.

ICO guidance requires organisations to record personal data breaches even where they decide that notification is not necessary.

Section 06

# NOTIFICATION AND COMMUNICATION

Meeting statutory duties. Informing appropriately. Communicating carefully.

External reporting and communication relating to personal data breaches will be coordinated through the Trust Data Protection Officer.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the breach must be notified to the Information Commissioner's Office without undue delay and, where feasible, no later than 72 hours after the organisation becomes aware of it. Where notification is made after 72 hours, the reasons for the delay must be provided.

The 72-hour period does not begin when the investigation is complete. The school must therefore report suspected breaches internally immediately so that Partnership Learning can assess the incident within the statutory timeframe.

Where the breach is unlikely to result in a risk to individuals' rights and freedoms, notification to the ICO is not required, but the breach and the reasons for that decision must still be documented.
Where a breach is likely to result in a high risk to affected individuals, those individuals must normally be informed without undue delay so that they can take appropriate steps to protect themselves.

Communication with affected individuals will be clear, proportionate and appropriate to their circumstances. Particular consideration will be given to the needs of pupils, families and individuals who may require accessible communication or additional support.

The Trust DPO will determine, in consultation with the school and other relevant professionals where necessary:

- whether notification to the ICO is required;
- whether affected individuals must or should be informed;
- whether another regulator, authority, police service, insurer or partner requires notification;
- what information should be communicated;
- the timing and method of communication.

Where safeguarding information has been compromised, the DSL will be involved in assessing and managing any safeguarding implications.

Section 07

# LEARNING FROM DATA BREACHES

Understanding causes. Strengthening safeguards. Preventing recurrence.

Riverside Bridge School will use personal data breaches and significant near misses as opportunities to strengthen information governance and reduce future risk.

Following an incident, the school will consider how the breach occurred, whether established procedures were followed, whether existing technical or organisational controls were sufficient and whether similar weaknesses could exist elsewhere.

Actions arising from review may include changes to systems, permissions, procedures, working practices, physical security, staff guidance or training.

Where appropriate, learning will be shared with relevant staff without unnecessarily identifying individuals involved in the original incident.

The purpose of review is not simply to identify individual error. The school will also consider whether systems, processes, workload, training, access arrangements or organisational controls contributed to the incident and whether wider improvement is required.

Repeated or recurring types of breach will be monitored so that patterns can be identified and addressed.

Section 08

# TRAINING AND AWARENESS

Building knowledge. Preventing breaches. Supporting confident reporting.

Effective prevention and response depend upon staff understanding both how to protect information and what to do when something goes wrong.

Staff, governors, volunteers and others who process personal information will receive information and training appropriate to their role. This will include the secure handling of personal information, recognising common breach scenarios, phishing and cyber-security threats, immediate reporting expectations and the importance of preserving confidentiality during an incident.

Staff will be reminded that reporting a potential breach promptly is always preferable to attempting to conceal, minimise or resolve an incident without appropriate support.

Refresher or targeted training will be provided where changes to legislation, technology, Trust arrangements or working practice make this necessary, and where incidents or monitoring identify a specific learning need.

Section 09

# MONITORING AND REVIEW

Monitoring incidents. Identifying trends. Strengthening practice.

The Headteacher has overall responsibility for ensuring that effective personal data-breach arrangements remain in place across Riverside Bridge School.

The School Data Protection Lead will maintain an appropriate confidential record of reported incidents and will monitor trends, recurring causes, response times and actions arising from breaches.

Monitoring will be used to identify whether particular systems, processes or areas of practice require further improvement and whether additional staff guidance, training or technical controls are needed.

Significant incidents, recurring patterns or material compliance concerns will be escalated appropriately to the Headteacher, Trust Data Protection Officer and Governing Board.

The Governing Board will receive appropriate assurance that:

- staff understand how to report suspected breaches;
- incidents are being managed appropriately;
- statutory notification arrangements are effective;
- actions arising from significant incidents are implemented;
- information-governance risks continue to be monitored.

This policy will be reviewed annually, or sooner where changes to legislation, regulatory guidance, Trust arrangements, technology or school operations make amendment necessary.

Section 10

# RELATED POLICIES & FRAMEWORKS

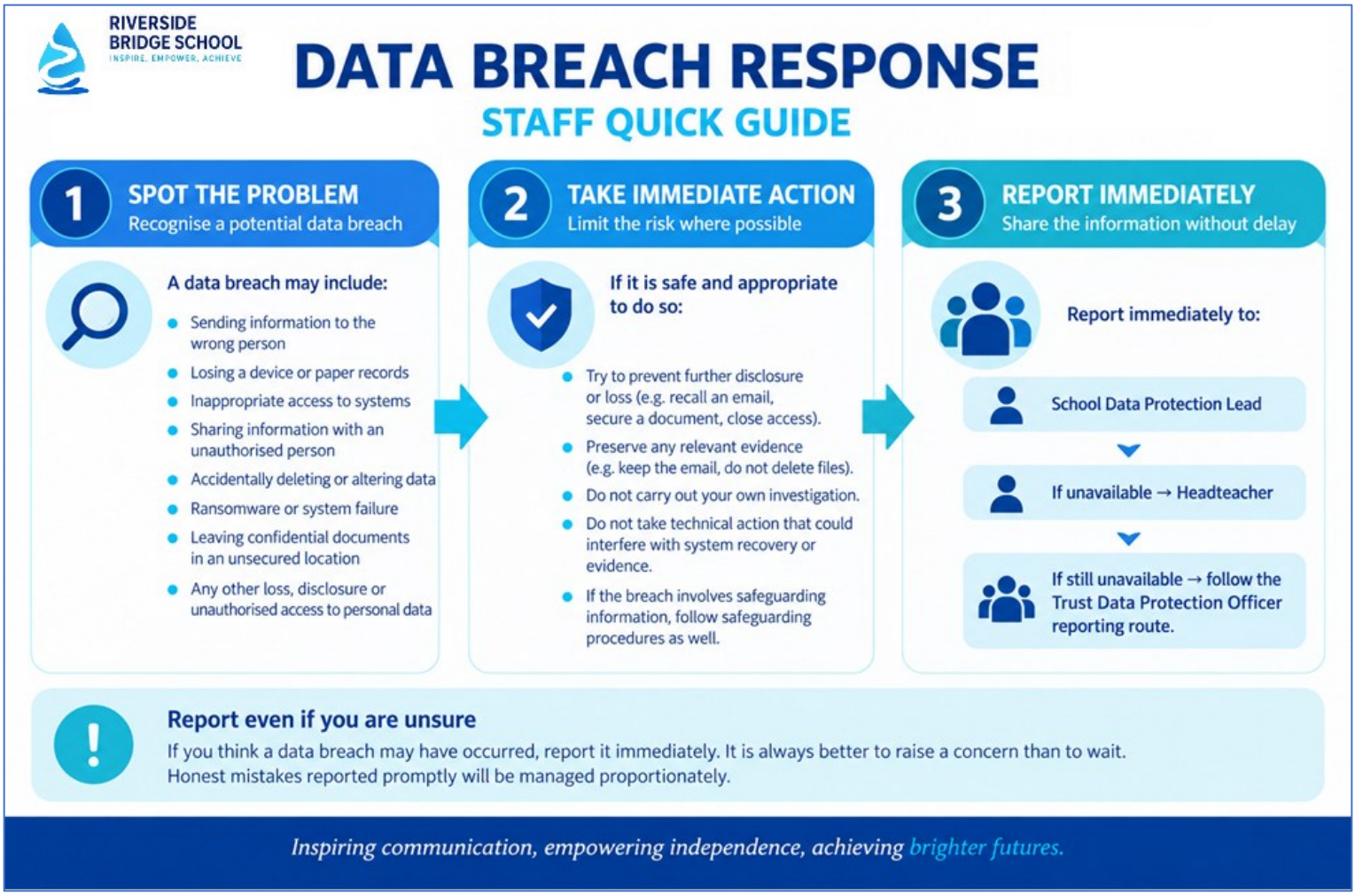
Connecting practice. Strengthening consistency.

This policy should be read alongside:

- Data Protection (GDPR) Policy
- Information Security Policy
- ICT Acceptable Use Policy
- Online Safety Policy
- Data Retention Policy
- Subject Access Request Policy
- Freedom of Information Policy
- CCTV Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Partnership Learning Data Breach Notification Policy
- relevant cyber-security and incident-response arrangements

Where a breach also constitutes a safeguarding, cyber-security, disciplinary, health and safety or other significant incident, the relevant policies and procedures will operate alongside this policy.

# APPENDIX


RIVERSIDE
BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE
DATA BREACH RESPONSE
STAFF QUICK GUIDE
1
SPOT THE PROBLEM
Recognise a potential data breach
A data breach may include:
Sending information to the wrong person
Losing a device or paper records
Inappropriate access to systems
Sharing information with an unauthorised person
Accidentally deleting or altering data
Ransomware or system failure
Leaving confidential documents in an unsecured location
Any other loss, disclosure or unauthorised access to personal data
2
TAKE IMMEDIATE ACTION
Limit the risk where possible
If it is safe and appropriate to do so:
Try to prevent further disclosure or loss (e.g. recall an email, secure a document, close access).
Preserve any relevant evidence (e.g. keep the email, do not delete files).
Do not carry out your own investigation.
Do not take technical action that could interfere with system recovery or evidence.
If the breach involves safeguarding information, follow safeguarding procedures as well.
3
REPORT IMMEDIATELY
Share the information without delay
Report immediately to:
School Data Protection Lead
If unavailable → Headteacher
If still unavailable → follow the Trust Data Protection Officer reporting route.
Report even if you are unsure
If you think a data breach may have occurred, report it immediately. It is always better to raise a concern than to wait.
Honest mistakes reported promptly will be managed proportionately.
Inspiring communication, empowering independence, achieving brighter futures.