INFORMATION SECURITY POLICY

Protecting information. Securing systems. 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 the confidentiality, integrity and availability of the information, systems and services used across the school. It establishes the responsibilities and safeguards required to protect information from unauthorised access, loss, alteration, disclosure, destruction or misuse.

Information is essential to safeguarding, teaching and learning, communication with families, school improvement and the effective operation of the school. Riverside Bridge School therefore recognises information security as an organisational responsibility that extends beyond ICT systems and applies whenever information is created, accessed, stored, shared, transported or disposed of.

The school will maintain proportionate technical, physical and organisational measures to manage information-security and cyber-security risks. These arrangements will reflect the sensitivity of the information being processed, the potential impact of loss or disruption, current legal and regulatory requirements and relevant national standards for schools.

Every member of staff, governor, volunteer, contractor and other authorised user has a responsibility to protect the information and systems they access. Staff will be supported through appropriate systems, procedures, training and guidance and are expected to report information-security concerns or suspected incidents promptly.

Our responsibilities to individuals

Riverside Bridge School will protect personal and confidential information throughout its lifecycle, restrict access to those with an appropriate need, maintain secure and resilient systems and take appropriate action where information or systems may have been compromised.

We will work with Partnership Learning, ICT providers and other relevant specialists to identify and manage security risks, maintain appropriate cyber-security controls, support recovery from incidents and continually strengthen our arrangements in response to changing risks and technology.

Through these commitments, Riverside Bridge School aims to ensure that information and systems remain secure, reliable and available to support pupils, staff and the effective operation of the school. We will continue to strengthen information security as an integral part of safeguarding, professional practice and organisational resilience.

RIVERSIDE BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE

TABLE OF CONTENTS

01	PURPOSE AND SCOPE	02	ROLES AND RESPONSIBILITIES
03	INFORMATION SECURITY PRINCIPLES	04	MANAGING INFORMATION SECURELY
05	PASSWORDS, AUTHENTICATION AND ACCESS CONTROL	06	EMAIL, INTERNET AND DIGITAL COMMUNICATIONS
07	MOBILE DEVICES, REMOTE AND HOME WORKING	08	PHYSICAL SECURITY AND PAPER RECORDS
09	CYBER SECURITY AND INCIDENT REPORTING	10	MONITORING AND REVIEW
11	RELATED POLICIES AND FRAMEWORKS		APPENDIX

APPROVED BY: Governing Board

APPROVED ON: September 2026

REVIEWED DUE ON: September 2027

Section 01

PURPOSE AND SCOPE

Defining expectations. Protecting information. Establishing secure practice.

The purpose of this policy is to establish a consistent approach to protecting information held by Riverside Bridge School. The policy aims to ensure that:

- information remains confidential where appropriate;
- information is accurate, complete and reliable;
- authorised users can access information when required;
- security risks are identified and managed;
- staff understand their responsibilities;
- the school complies with legal, regulatory and contractual requirements.

The policy supports all information processed by the school, regardless of whether it is held electronically, on paper or in any other format.

This policy applies to all individuals who access, process or manage information on behalf of Riverside Bridge School, including employees, governors, volunteers, agency staff, contractors, trainees, students on placement and any other authorised users of school information or systems.

It applies to all information processed by the school, including:

- pupil information;
- safeguarding records;
- SEND documentation;
- staff information;
- financial information;
- governance records;
- emails and electronic communications;
- photographs and videos;
- paper records;
- information stored within cloud-based or third-party systems approved for school use.

Section 02

ROLES AND RESPONSIBILITIES

Clarifying accountability. Sharing responsibility. Maintaining oversight.

Protecting information is the responsibility of everyone working at Riverside Bridge School. Effective information security depends upon appropriate leadership, secure systems and the day-to-day actions of every individual who handles school information.

The Governing Board is responsible for ensuring that appropriate information security arrangements are in place across the school. It will:

- receive assurance that information security risks are being managed effectively;
- support compliance with legal and regulatory requirements;
- ensure appropriate policies are maintained;
- monitor the effectiveness of the school's information governance arrangements.

The Headteacher has overall responsibility for the implementation of this policy and for promoting a culture in which information security is understood as an essential part of safeguarding, leadership and professional practice. The Headteacher will ensure that:

- appropriate technical and organisational measures are in place;
- information security risks are considered as part of school decision-making;
- staff receive appropriate training and guidance;
- security incidents are investigated promptly; and
- improvements are implemented following reviews or incidents.

The School Data Protection Lead will oversee the school's day-to-day information governance arrangements by:

- providing advice and guidance to staff;
- monitoring compliance with this policy;
- coordinating responses to information security incidents;
- supporting investigations into data breaches;
- liaising with ICT providers and external agencies where required; and
- reviewing security procedures in response to changing risks.

Every member of staff has a personal responsibility to protect the information they access or process during their work. Staff are expected to:

- handle information securely at all times;
- protect passwords and login credentials;
- use only approved school systems and devices;
- report security concerns immediately;
- follow school policies and procedures;
- complete required information security training.

Information security is everyone's responsibility and forms part of the school's wider safeguarding culture.

Partnership Learning ICT Team supports the school in maintaining secure, resilient and appropriately managed digital systems in accordance with its respective responsibilities and service arrangements. This includes, where applicable:

- maintaining appropriate network and system security controls;
- managing security updates, vulnerability remediation and supported software;
- maintaining appropriate anti-malware, firewall and other protective technologies;
- supporting secure account, authentication and access-control arrangements;
- maintaining appropriate backup and recovery arrangements;
- monitoring and responding to identified technical security threats;
- supporting investigation, containment and recovery following cyber-security incidents;
- providing specialist advice to the school on emerging risks and required security improvements.

The Headteacher and School Data Protection Lead will work with the Trust ICT Team to obtain appropriate assurance that technical security arrangements remain effective and proportionate.

Section 03

INFORMATION SECURITY PRINCIPLES

Protecting confidentiality. Maintaining integrity. Ensuring availability.

The school's approach to information security is based on three fundamental principles.

Confidentiality

Information should only be accessed by individuals who have a legitimate need to see it as part of their role. The school will ensure that:

- access is restricted appropriately;
- confidential information is shared only where necessary;
- sensitive information is protected during storage and transmission;
- staff understand their responsibilities regarding confidentiality.

Integrity

Information must remain accurate, complete and reliable throughout its lifecycle. The school will:

- maintain accurate records;
- protect information from unauthorised alteration;
- ensure changes are made only by authorised individuals;
- maintain appropriate version control where required.

Availability

Information must be available to authorised users when it is needed to support education, safeguarding and school operations. The school will therefore:

- maintain secure information systems;
- support appropriate backup and recovery arrangements;
- minimise unnecessary disruption;
- work with ICT providers to maintain resilient systems.

These principles underpin all aspects of the school's information governance arrangements and should be considered whenever information is created, accessed, shared, stored or disposed of.

Section 04

MANAGING INFORMATION SECURELY

Handling carefully. Sharing appropriately. Protecting confidentiality.

Every member of staff is responsible for handling information in a way that protects confidentiality while supporting the effective operation of the school.

Information should only be collected, accessed and shared where there is a legitimate educational, safeguarding or operational reason for doing so.

Staff should always consider whether the information is necessary, the recipient is authorised to receive it, the method of sharing is secure and the information is being stored appropriately.

Information must not be:

- accessed out of curiosity;
- shared with unauthorised individuals;
- removed from the school without appropriate authorisation;
- stored on unapproved personal devices or cloud storage services;
- left unattended where unauthorised individuals could access it.

When handling confidential information, staff should take reasonable steps to protect privacy, particularly in shared offices, classrooms, public areas and during meetings with parents, professionals or visitors.

Particular care should be taken when working with:

- safeguarding information;
- Education, Health and Care Plans (EHCPs);
- medical information;
- personnel records;
- financial information;
- any information classified as confidential or special category personal data.

The school recognises that effective information security is achieved through good professional judgement, supported by clear procedures, rather than relying solely on technical controls.

Systems and services used to create, store, access or share school information must be approved for school use. Staff must not introduce new applications, cloud services, artificial-intelligence tools or other digital services for processing confidential or personal information unless they have been appropriately approved in accordance with school and Trust arrangements. Where third-party systems process school information, appropriate consideration will be given to information security, data protection, access controls, contractual arrangements and the risks associated with the information being processed.

Section 05

PASSWORDS, AUTHENTICATION AND ACCESS CONTROL

Controlling access. Strengthening authentication. Protecting accounts.

Secure authentication is one of the most effective ways of protecting the school's information and systems. All users are responsible for ensuring that their login credentials remain secure and are not shared with others.

The school will implement appropriate access controls so that staff are only able to access the information and systems necessary for their role. Access permissions will be reviewed periodically and amended promptly when staff change roles or leave the organisation.

Staff are expected to:

- create strong passwords in accordance with school and Trust ICT requirements;
- keep passwords confidential and never share them with colleagues or pupils;
- use multi-factor authentication (MFA) where required by the school, Trust or system provider, and particularly for systems or accounts where enhanced authentication is required as part of the school's security arrangements;
- lock computers or devices whenever they are left unattended;
- log out of systems when work is complete, particularly on shared devices;
- report any suspected compromise of login credentials immediately.

Under no circumstances should staff:

- write passwords where they are visible to others;
- allow another person to use their account;
- attempt to access systems using another person's credentials;
- use shared accounts unless specifically authorised for operational reasons.

Protecting login credentials is an essential safeguard against unauthorised access to confidential information.

User accounts will be created, amended, suspended and removed promptly to reflect an individual's role and current authority. Privileged or administrative access will be restricted to those who require it and subject to appropriate additional controls. Default, dormant and unnecessary accounts will be removed, disabled or otherwise secured as appropriate.

Section 06

EMAIL, INTERNET AND DIGITAL COMMUNICATIONS

Communicating securely. Recognising threats. Preventing disclosure.

Email and digital communication systems are essential tools for the effective operation of the school. However, they also present one of the greatest information security risks if used inappropriately.

Staff should ensure that information is shared only with appropriate recipients and using approved school systems.

Before sending emails containing confidential or personal information, staff should take a moment to confirm:

- the recipient's email address is correct;
- attachments contain the intended information;
- confidential information is being shared only where there is a legitimate need;
- the level of security is appropriate for the information being sent;
- the content is accurate and professional.

Staff should not:

- use personal email accounts for school business;
- forward confidential information to unauthorised individuals;
- click links or open attachments from suspicious or unexpected emails;
- use unapproved messaging applications to share confidential information;
- download software or files from untrusted sources.

The school recognises that cyber threats continue to evolve. Staff should remain vigilant for phishing emails, fraudulent requests, fake websites and other attempts to obtain confidential information. Any suspicious communications should be reported immediately to the School Data Protection Lead or ICT support.

Appropriate use of email and digital communication supports safeguarding, protects personal information and helps maintain public confidence in the school.

Section 07

MOBILE DEVICES, REMOTE AND HOME WORKING

Working securely. Protecting devices. Maintaining confidentiality.

Riverside Bridge School recognises that staff may occasionally access school information away from the school site as part of their professional responsibilities.

When working remotely, staff remain responsible for protecting school information to the same standard expected within school.

Staff should:

- use only approved school devices or authorised systems wherever possible;
- ensure devices are protected with passwords or biometric security;
- keep devices with them or securely stored at all times;
- avoid discussing confidential information in public places;
- ensure screens cannot easily be overlooked by others when working outside school;
- securely store paper records during transport and home working;
- return confidential information to school promptly when no longer required.

Staff should not:

- leave school devices or confidential information unattended in vehicles except where this is unavoidable, brief and appropriate security measures have been taken;
- store confidential school information on personal cloud storage services;
- allow family members or other individuals to access school devices;
- print confidential information at home unless authorised and appropriate security arrangements are in place;
- dispose of confidential papers through household waste.

The school understands that flexible and remote working can support operational effectiveness. However, this must never compromise the security of school information or the privacy of individuals.
Loss or theft of any device or information used for school purposes must be reported immediately in accordance with the school's incident-reporting arrangements.

Section 08

PHYSICAL SECURITY AND PAPER RECORDS

Securing records. Controlling access. Protecting information.

Whilst much of the school's information is held electronically, paper records continue to form an important part of school operations, particularly within safeguarding, SEND and administrative functions.
Paper records require the same level of protection as electronic information.

Staff are expected to:

- store confidential records securely when not in use;
- collect printing promptly from printers and photocopiers;
- use confidential waste facilities for sensitive documents;
- keep desks and shared workspaces clear of confidential information when unattended;
- ensure visitors cannot view confidential information inadvertently;
- report lost or misplaced documents immediately.

Particular care should be taken when handling:

- safeguarding files;
- EHCP documentation;
- medical information;
- behaviour records;
- personnel files;
- financial documentation.

Maintaining a secure working environment helps protect individuals, reduces the risk of data breaches and supports the school's wider safeguarding responsibilities.

Section 09

CYBER SECURITY AND INCIDENT REPORTING

Recognising threats. Reporting promptly. Supporting recovery.

Cyber security is an essential part of protecting Riverside Bridge School's information, systems and services. A cyber incident may compromise confidential or personal information, disrupt safeguarding and communication systems, interrupt teaching and learning or affect the school's ability to operate safely and effectively.

The school will take a proportionate, risk-based approach to cyber security and will work with Partnership Learning and approved ICT providers to maintain appropriate technical and organisational safeguards. These arrangements will reflect current risks, the sensitivity and importance of the information and systems being protected, and relevant national standards for schools.

Cyber-security arrangements

Riverside Bridge School will maintain arrangements designed to prevent, detect, respond to and recover from cyber-security incidents. These will include, as appropriate:

- regular assessment and review of cyber-security risks;
- appropriate firewall, anti-malware and endpoint protection;
- secure configuration of networks, systems and devices;
- timely application of security updates and remediation of identified vulnerabilities;
- use of supported and appropriately licensed software;
- secure management of user accounts, access permissions and privileged accounts;
- multi-factor authentication and other enhanced authentication controls where required;
- appropriate filtering and monitoring arrangements;
- secure backup and recovery arrangements;
- appropriate controls for removable storage and external devices;
- management of information-security risks associated with third-party systems and services;
- arrangements for containing, investigating and recovering from cyber-security incidents.

Cyber-security controls will be reviewed in response to changes in systems, identified vulnerabilities, significant incidents, emerging threats and relevant national guidance.

Backups and recovery

The school will ensure that important information and systems are subject to appropriate backup and recovery arrangements. Backup arrangements will reflect the importance and sensitivity of the information

concerned and the impact that its loss or unavailability could have on safeguarding, education and school operations.

Partnership Learning and ICT providers will support the school in ensuring that backup arrangements are appropriately secured, maintained and tested and that the school has sufficient assurance that critical information can be restored following accidental loss, system failure or cyber attack.

Backup and recovery arrangements will link to the school's Emergency Management and Business Continuity Plan and associated disaster-recovery arrangements.

Recognising cyber-security concerns

Every member of staff has a responsibility to remain alert to potential cyber threats and to report concerns promptly. Staff are not expected to diagnose or investigate technical incidents themselves.

Indicators of a potential cyber-security incident may include:

- phishing, suspicious or unexpected emails;
- unexpected requests for passwords, authentication codes, personal or financial information;
- suspicious multi-factor authentication requests;
- unusual computer, account or network activity;
- ransomware, malware or security alerts;
- unexpected changes to files or systems;
- loss of access to systems or information;
- suspected unauthorised access to an account or system;
- lost or stolen devices containing or providing access to school information;
- accidental or unauthorised disclosure of confidential information;
- suspicious websites, links, downloads or attachments;
- any other activity that suggests school information, accounts, devices or systems may have been compromised.

Staff should treat unexpected requests for information, payments, changes to bank details, passwords or authentication as potentially suspicious and verify them through an appropriate independent route before taking action.

Responding to a suspected cyber-security incident

Where a member of staff suspects that a cyber-security incident has occurred, they must report it immediately through the school's agreed ICT reporting arrangements.

Where personal or confidential information may have been compromised, the School Data Protection Lead must also be informed so that the incident can be considered under the Data Breach Response Policy.

Staff should:

- stop the activity that may be contributing to the incident where it is safe and appropriate to do so;
- report the concern promptly and provide clear factual information about what has occurred;
- preserve relevant emails, messages, screenshots or other information where this can be done safely;
- follow instructions provided by ICT Support, the School Data Protection Lead or senior leadership;
- remain alert to further suspicious activity.

Staff must not independently investigate a cyber incident, install software, attempt technical repairs, delete potentially relevant information or take other action that could interfere with the investigation or recovery process. Where there is uncertainty about whether something constitutes a cyber-security incident, staff should report the concern rather than delay.

Managing and escalating incidents

The school will work with Partnership Learning, approved ICT providers and other relevant specialists to assess suspected cyber incidents and determine the appropriate response.

Depending upon the nature and severity of the incident, action may include:

- containing affected accounts, devices or systems;
- protecting critical information and services;
- resetting or securing compromised credentials;
- assessing whether personal information has been affected;
- activating data-breach procedures;
- restoring information or systems from secure backups;
- activating business-continuity or disaster-recovery arrangements;
- communicating with affected individuals or stakeholders where appropriate;
- notifying relevant external organisations or authorities where required;
- recording and reviewing the incident to identify lessons and required improvements.

Decisions about external reporting will be made by the appropriate school, Trust or specialist lead in accordance with the nature of the incident and applicable legal, regulatory, contractual or insurance requirements.

Learning and resilience

Following a significant cyber-security incident, the school will review what occurred, the effectiveness of its response and whether changes are required to systems, controls, procedures, training or working practices. Lessons identified through incidents, near misses, risk assessments, technical reviews and emerging threats will inform the continuing development of the school's information-security arrangements. Cyber security will be considered alongside information governance, safeguarding, risk management and business continuity so that the school can protect information while maintaining access to the systems and services required to support pupils and operate effectively.

Section 10

MONITORING AND REVIEW

Monitoring security. Learning from incidents. Strengthening resilience.

The Headteacher has overall responsibility for ensuring that effective information security arrangements are maintained across Riverside Bridge School.

The School Data Protection Lead will:

- monitor compliance with this policy;
- review information security incidents and identify trends;
- support staff through advice, guidance and training;
- coordinate responses to information security concerns;
- work with ICT providers to improve security arrangements;
- review procedures in response to legislative, technological or organisational change.

Information security will form part of the school's wider programme of information governance, safeguarding and risk management.

The school will ensure that cyber-security risks are assessed and reviewed in accordance with current DfE standards and Trust arrangements. Identified risks, vulnerabilities, incidents and required improvements will inform the school's wider risk-management and digital-development arrangements.

The Governing Board will receive assurance that:

- appropriate information security arrangements remain in place;
- significant information security risks are being managed appropriately;
- staff receive appropriate training and support;
- the school continues to comply with its legal and regulatory responsibilities.

This policy will be reviewed annually, or sooner where changes to legislation, technology or operational requirements make this necessary.

Section 11

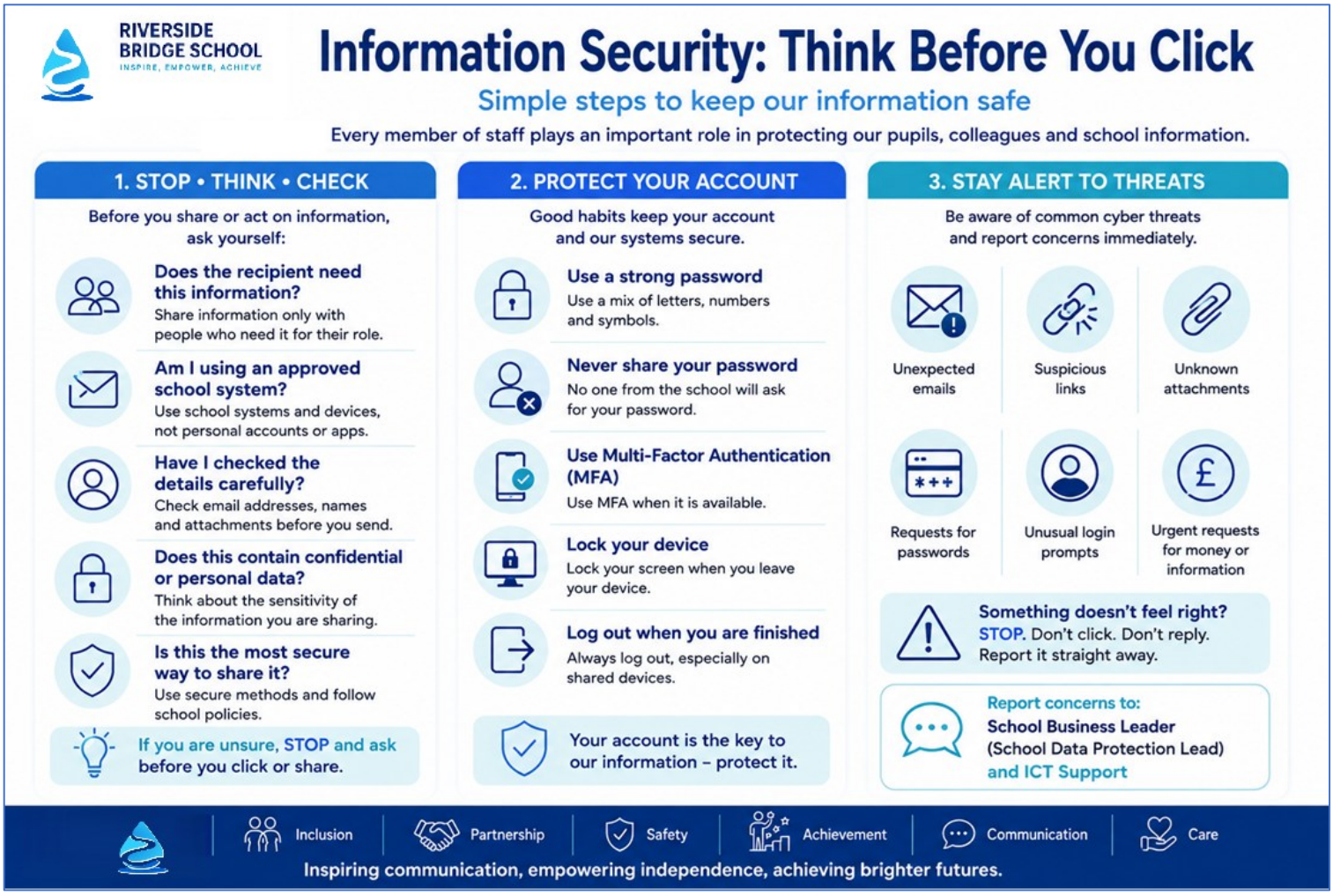
RELATED POLICIES & FRAMEWORKS

Connecting practice. Strengthening consistency.

This policy should be read alongside:

- Data Protection (GDPR) Policy
- Data Breach Response Policy
- Data Retention Policy
- Subject Access Request Policy
- Freedom of Information Policy
- CCTV Policy
- Privacy Notices
- Online Safety Policy
- ICT Acceptable Use Policy
- Staff Code of Conduct
- Safeguarding and Child Protection Policy
- Risk Management and Risk Assessment Policy
- Emergency Management and Business Continuity Plan

APPENDIX


RIVERSIDE BRIDGE SCHOOL
INSPIRE, EMPOWER, ACHIEVE
Information Security: Think Before You Click
Simple steps to keep our information safe
Every member of staff plays an important role in protecting our pupils, colleagues and school information.
1. STOP • THINK • CHECK
Before you share or act on information, ask yourself:
Does the recipient need this information?
Share information only with people who need it for their role.
Am I using an approved school system?
Use school systems and devices, not personal accounts or apps.
Have I checked the details carefully?
Check email addresses, names and attachments before you send.
Does this contain confidential or personal data?
Think about the sensitivity of the information you are sharing.
Is this the most secure way to share it?
Use secure methods and follow school policies.
If you are unsure, STOP and ask before you click or share.
2. PROTECT YOUR ACCOUNT
Good habits keep your account and our systems secure.
Use a strong password
Use a mix of letters, numbers and symbols.
Never share your password
No one from the school will ask for your password.
Use Multi-Factor Authentication (MFA)
Use MFA when it is available.
Lock your device
Lock your screen when you leave your device.
Log out when you are finished
Always log out, especially on shared devices.
Your account is the key to our information – protect it.
3. STAY ALERT TO THREATS
Be aware of common cyber threats and report concerns immediately.
Unexpected emails
Suspicious links
Unknown attachments
Requests for passwords
Unusual login prompts
Urgent requests for money or information
Something doesn't feel right?
STOP. Don't click. Don't reply. Report it straight away.
Report concerns to:
School Business Leader
(School Data Protection Lead)
and ICT Support
Inclusion
Partnership
Safety
Achievement
Communication
Care
Inspiring communication, empowering independence, achieving brighter futures.