SPAGHETTI BRIDGE

Cyber Security Policy

November 2025

Policy Owner	Group Head of IT and Systems
Applies to	The policy will apply to all school staff and all group staff
Associated Documents	Acceptable Use Policy
Review Frequency	Annually
Review Date	June 2026
New Review Date	June 2027
Approved by Chief Executive Officer	Dan Alipaz Dan Alipaz (Jun 25, 2026, 9:39am)
Approved by the Chair of the Board	Stephen Bradshaw Stephen Bradshaw (Jun 22, 2026, 11:08am)

Table of Contents

---

1. Introduction and Scope

This Cyber Security Policy establishes the framework for protecting digital assets, data, and systems across all schools within our School Group. This policy applies to all individuals who access our IT systems and data, including students, teaching staff, support staff, caretakers, contractors, and head office personnel.

The policy ensures compliance with UK legislation including the Data Protection Act 2018, UK GDPR, Computer Misuse Act 1990, and guidance from the Department for Education and National Cyber Security Centre (NCSC).

Disciplinary action may be taken for non-compliance with this policy.

2. Definitions

Acceptable Use Policy (AUP): Guidelines that define appropriate and inappropriate use of an organisation's IT resources, networks, and systems.

Authentication App: A software application that generates time-based one-time passwords (TOTP) or push notifications for multi-factor authentication, such as Microsoft Authenticator, Google Authenticator, or similar approved applications.

Business Continuity: The capability of an organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

Cloud Service Provider: External organisations that provide computing resources, software applications, or storage services via the internet, such as Google Workspace, Microsoft 365, or educational platforms.

Critical Systems: IT systems essential for school operations, including student information management systems, financial systems, communication platforms, safeguarding databases, and any system whose failure would significantly impact educational delivery or student/staff safety.

Cyber Safe Team: The designated group of professionals responsible for incident response, security monitoring, and cyber security coordination across the school group, contactable at cyber_safe@spbridge.co.uk.

Data Breach: Any incident where personal data is accidentally or unlawfully destroyed, lost, altered, disclosed, or accessed without authorisation, regardless of whether the data was encrypted or otherwise protected.

Data Classification: The process of organising data into categories based on sensitivity levels and business requirements to ensure appropriate protection measures are applied.

Data Loss Prevention (DLP): Technologies and processes designed to detect and prevent unauthorised use, transmission, or disclosure of sensitive information.

Data Processing Agreement (DPA): A legal contract between a data controller and data processor that governs the processing of personal data and ensures GDPR compliance.

Data Protection Impact Assessment (DPIA): A systematic process to identify and minimise data protection risks, required for high-risk processing activities under GDPR.

Digital Citizenship: The responsible and ethical use of technology, encompassing online safety, digital literacy, and appropriate behaviour in digital environments.

DPIA: Data Protection Impact Assessment is a process used to identify and mitigate risks to privacy and security when processing personal data. It helps organisations understand and address potential harms to individuals' rights and freedoms when new or modified systems or processes involve personal data.

Endpoint: Any device that connects to the school network, including computers, laptops, tablets, smartphones, interactive whiteboards, printers, and IoT devices.

Incident: Any event that could compromise the confidentiality, integrity, or availability of information or systems.

Insider Threat: The potential for individuals with authorised access to use their access maliciously or accidentally cause harm to the organisation's information systems or data.

IT and Systems Team: Personnel with administrative or technical responsibilities for school IT systems, including the Group Head of IT and Systems, system administrators, network administrators, technical support staff, and any contractors or third parties with elevated system privileges.

Leavers Form: The mandatory automated system used to process all staff departures and ensure timely termination of access rights to protect organisational security and data.

Multi-Factor Authentication (MFA): A security process that requires users to provide two or more verification factors to gain access to systems, combining something they know (password), something they have (authentication device), and/or something they are (biometric verification).

Network Segmentation: The practice of dividing a computer network into smaller segments or subnets to improve security, performance, and management by controlling traffic flow between different areas of the network.

Personal Data: Any information relating to an identified or identifiable individual, including students, staff, and parents.

Phishing: Fraudulent attempts to obtain sensitive information such as usernames, passwords, or financial details by impersonating trustworthy entities in electronic communications.

Privacy by design: Privacy by Design is a framework that embeds privacy considerations into the development and operation of systems, technologies, and business practices from the very beginning, rather than adding privacy protections as an afterthought.

Privileged Access: Elevated system permissions that allow users to perform administrative functions, modify system configurations, access sensitive data beyond their normal role requirements, or perform actions that could affect system security or availability.

Ransomware: Malicious software that encrypts files or systems and demands payment for their recovery, representing a significant threat to educational institutions and their data.

Recovery Point Objective (RPO): The maximum acceptable amount of data loss measured in time, representing how much data can be lost before it significantly impacts operations.

Recovery Time Objective (RTO): The maximum acceptable length of time that a system can be offline after a failure or disaster occurs.

Response: The process of identifying, managing, and recovering from a cybersecurity incident or breach. It's essentially how an organization reacts when something goes wrong security-wise - like a data breach, malware infection, ransomware attack, or unauthorised access.

Secure handling: The practice of protecting digital information throughout its entire lifecycle by implementing appropriate access controls, encryption, backup procedures, and disposal methods to prevent unauthorised access, disclosure, modification, or destruction while ensuring data availability for legitimate business purposes.

Single Sign-On (SSO): An authentication process that allows users to access multiple applications with one set of login credentials, improving both security and user experience.

Social Engineering: Psychological manipulation techniques used to trick individuals into divulging confidential information or performing actions that compromise security.

Special Category Data: Sensitive personal data including health records, safeguarding information, and data relating to a child's special educational needs.

System Users: All individuals granted access to school IT systems, including networks, devices, applications, and data.

Vulnerability: A weakness in a system, application, or process that could be exploited by threats to gain unauthorised access or cause harm to information or systems.

Zero Trust: A security model that requires verification of every user and device attempting to access systems, regardless of their location or previous access history.

3. Roles and Responsibilities

3.1 Cyber-Safe Team

- Overall accountability for cyber security across the school group
- Ensuring adequate resources for cyber security measures
- Approving cyber security policies and procedures
- Reporting significant incidents to relevant authorities

Section 3.1.1 Patch Management Timelines:

- Critical and high-risk security updates must be installed within 14 days of release
- This includes operating system patches, application security updates, and firmware for network devices (firewalls, routers, switches)

- Security updates take priority over feature updates or optional patches
- Patch severity ratings should follow vendor classifications (Critical, High, Medium, Low)
- Emergency patches for actively exploited vulnerabilities must be prioritised and may require out-of-hours deployment
- Patch compliance must be monitored and reported monthly
- Any systems unable to meet the 14-day requirement must be documented with compensating controls or remediation plans

3.2 Group Head of IT and Systems

- Day-to-day management of cybersecurity
- Implementation and maintenance of technical security controls
- Managing user access provisioning and deprovisioning procedures
- Ensuring immediate account deactivation upon staff departure
- Leading incident response activities as part of the Cyber Safe team
- Coordinating external escalations to cyber_safe@spbridge.co.uk and regulatory authorities
- Regular security assessments and updates

3.3 Data Protection Officer (DPO)

- The company GDPR Sentry act as our DPO

3.4 School Leadership Team

- Implementing cyber security measures within their school
- Ensuring staff compliance with policies
- Receiving and assessing initial cyber security incident reports from school staff
- Making escalation decisions to notify the Cyber Safe team
- Reporting security incidents to cyber_safe@spbridge.co.uk within required timeframes
- Promoting cyber security awareness among students and staff

4. User Categories and Access Controls

4.1 Students

Access Level: Restricted educational access

Permitted Activities:

- Accessing approved educational resources and platforms
- Storing schoolwork on designated network areas
- Using educational software and applications

Prohibited Activities:

- Installing unauthorised software or applications
- Accessing inappropriate or harmful content
- Sharing login credentials with others
- Attempting to bypass security controls
- Accessing staff-only systems or data

Security Requirements:

- Unique login credentials for each student
- Strong passwords meeting minimum complexity requirements (8 characters, mixed case, numbers, special characters)
- Age-appropriate internet filtering and monitoring on all accessible equipment
- Annual password changes
- Digital citizenship education and training
- Students will have MFA enforced
- Passwords must be changed immediately if they are believed to be compromised and the IT and System team informed
- If data is to be stored on the student's device then the media must be secured with Microsoft Bitlocker Encryption
- Default passwords on systems are immediately changed
- Installation of un-approved software or code is not permitted without permission

4.2 School Staff (SLT, Admin and Teaching)

Access Level: Practitioner-level educational systems access

System Access:

- All elements of BridgeLink
- Educational platforms and learning management systems
- Assessment and reporting tools
- Communication systems (GMail, Google Chat, Google Meets, other messaging) - other email clients are not permitted

Data Access Boundaries:

- Access restricted to data for their specific school only
- Student data limited to classes/groups in their school
- Historical data access as required for educational continuity
- No access to financial, HR, or operational data from other schools

Permitted Activities:

- Accessing student information systems for educational purposes
- Using approved educational technology platforms
- Storing and processing student data in accordance with data protection requirements
- Accessing professional development resources

Security Requirements:

- Strong passwords meeting minimum complexity requirements (password strength to be aligned with Google's specification of a 'Strong' password)
- Multi-factor authentication mandatory on all staff accounts
- Regular security awareness training
- Secure handling of student data
- Immediate reporting of security incidents in line with the cyber security Response detailed in this policy

- Passwords must be changed immediately if they are believed to be compromised and the IT and System team informed
- If data is to be stored on the staff member's device then the media must be secured with Microsoft Bitlocker Encryption

- Default passwords on systems are immediately changed

- Installation of software or code is not permitted without permission

4.3 Caretakers and Facilities Staff

Access Level: Limited access for operational requirements

Permitted Activities:

- Accessing building management systems as required
- Using designated communication systems
- Basic administrative system access where necessary

Security Requirements:

- Minimal necessary access to IT systems
- Strong passwords meeting minimum complexity requirements (password strength to be aligned with Google's specification of a 'Strong' password)
- Supervised access to sensitive areas containing IT equipment
- Basic cyber security awareness training delivered annually
- Clear procedures for reporting IT-related issues
- Passwords must be changed immediately if they are believed to be compromised and the IT and Systems team informed using the cyber_safe@spbridge.co.uk email address
- If data is to be stored on the staff member's device then the media must be secured with Microsoft Bitlocker Encryption
- Default passwords on systems are immediately changed

- Installation of software or code is not permitted without permission

4.4 Contractors and Third Parties

Access Level: Strictly controlled and monitored access

Requirements:

- Signed data processing agreements before access
- Data Protection Impact Assessment (DPIA) completed for all cloud suppliers and service providers
- Background checks where appropriate
- All access requests must be authorised by both the contracting manager and relevant system owner
- Access granted on minimum necessary basis only
- Supervised access to school premises and systems
- Temporary access credentials with defined expiry dates
- Compliance with school cyber security standards
- Immediate revocation of access upon contract completion or termination
- No usage of external media or devices is permitted without the written approval of a member of the Cyber Safe team. This includes but is not limited to USB drives (whether encrypted or not), portable hard-drives, optical disk media or direct laptop connections. HDMI connections are allowed if a member of the school/group staff oversees the implementation.
- All contractors must be shown our cyber security policy and communicate that they have read it and will comply. Records of this will be kept in our supplier records
- Default passwords on systems are immediately changed

4.5 Group Personnel

Access Level: Cross-school administrative access with departmental restrictions

System Access:

- Access to multiple services in BridgeLink
- Group-wide financial and administrative systems
- HR management systems across all schools
- Service development, Facilities and estates management systems
- Group reporting and analytics platforms

Data Access Boundaries:

- Access spans all schools within Spaghetti Bridge Ltd
- Data access restricted to specific departmental functions only (e.g., Finance staff access financial data only, HR staff access personnel data only)
- Access by default is limited by department. Cross-departmental access requires senior management approval

- Enhanced monitoring and audit logging for cross-school access
- If data is to be stored on the staff member's device then the media must be secured with Microsoft Bitlocker Encryption

Security Requirements:

- Enhanced authentication measures with mandatory MFA
- Strong passwords meeting minimum complexity requirements (password strength to be aligned with Google's specification of a 'Strong' password)
- Regular security clearance reviews
- Access to cross-school management systems
- Elevated security training requirements
- Comprehensive audit logging of activities
- Passwords must be changed immediately if they are believed to be compromised and the IT and System team informed
- Default passwords on systems are immediately changed
- Installation of software or code is not permitted without permission

5. Technical Security Controls

5.1 Network Security

- Firewall protection on all network perimeters
- Secure Wi-Fi networks with WPA3 encryption at each site
- Regular network security assessments
- Intrusion detection and prevention systems in network and IT areas

Firewall Configuration Management

- Opening ports on the firewall requires a business case signed off by the Group Head of IT and Systems and documented in the Team Vault application
- Outside configuration of our firewalls is permitted only when the Group Head of IT and Systems has signed off the need for this to happen along with a documented business case

5.2 Endpoint Security

- Antivirus software on all devices
- Security patches must be applied within 14 days of release for critical and high-severity vulnerabilities
- Regular security updates and patch management with documented approval processes
- No use of unencrypted media
- Remote wipe capabilities for mobile devices

- USB port controls and data loss prevention

Approved Web Browsers:

- Only approved and supported web browsers may be used to access school systems and data, approved browsers include: Google Chrome and Microsoft Edge
- Browsers must be kept up-to-date with automatic updates enabled
- Browser extensions and plugins require IT approval before installation
- Private/incognito browsing must not be used to bypass security controls
- Browser security settings must not be disabled or weakened
- Unsupported or end-of-life browsers are prohibited
- Removable Media Testing
- All removable media (USB drives, external hard drives, optical disks, etc.) received from external sources must be tested on a dedicated, non-network-connected device before being connected to any school or group system.

Only the designated isolated testing device may be used for this purpose. This device must:

- Have no network connectivity (wired or wireless)
- Be maintained and updated by the IT and Systems Team
- Have up-to-date antivirus and malware scanning software
- Be regularly wiped and rebuilt to maintain security integrity
- No removable media may be connected to network-connected systems without prior scanning and approval from a member of the IT and Systems Team.

Device Locking and Physical Security

- All devices must have screen/device locking enabled
- Devices must automatically lock after a maximum of 15 minutes of inactivity
- Acceptable unlock methods: passwords, PINs, biometric authentication (fingerprint, facial recognition)
- Users must manually lock devices when leaving them unattended
- Lost or stolen devices must be reported immediately to IT via the cyber_safe@spbridge.co.uk email address

Host-based Firewall Protection

- Windows Firewall (or equivalent host-based firewall) must be enabled on all devices
- Users must not disable or deactivate Windows Firewall
- Firewall exceptions must be approved by IT and documented
- Regular audits will be held to verify firewall status across all endpoints

5.3 Access Management

5.3.1 User Account Provisioning

- All user accounts must follow a formal approval process and adhere to the principle of least privilege:

  User Account Creation Process:

- All user accounts must follow a formal approval process before creation
- New user account requests must be submitted through IT with appropriate business justification
- Account creation must be authorised by the user's line manager or department head
- HR must confirm the individual's employment status and role before accounts are provisioned
- Access rights must be assigned based on the approved job role and follow the principle of least privilege
- All account creation requests and authorisations must be documented and retained
- Accounts must only be created after successful completion of the approval workflow
- Temporary or contractor accounts must have defined expiry dates aligned with their contract period
- Access is only granted on a 'least access required' basis and accounts will only be given the minimum access that they need to perform their role

5.3.2 Ongoing Access Controls

- Role-based access controls (RBAC) with system access limited to job requirements only
- Data access restricted by organisational boundary (school-specific or department-specific)
- All system access granted on a need-to-know basis only
- Immediate disabling of user accounts upon termination of employment or contract
- Strong passwords meeting minimum complexity requirements (password strength to be aligned with Google's specification of a 'Strong' password)
- Single sign-on (SSO) where possible
- Passwords must be changed immediately if they are believed to be compromised and the IT and System team informed using the cyber_safe@spbridge.co.uk email address
- Areas that store physical hardware will be secured with access only given to the IT and Systems team and other personnel on a recorded basis. The Team Vault app stores access to these locations
- Default passwords on systems and hardware are immediately changed
- No staff are permitted to store Spaghetti Bridge data on any unencrypted media

5.3.3 Multi-Factor Authentication (MFA) Requirements

Standard MFA for All Staff:

- Multi-factor authentication (MFA) mandatory for all staff and student GMail accounts
- MFA required for access to all school systems, email, and cloud services where available if the system allows access to:
    - Remote access (VPN)
    - Administrative accounts
    - Access to sensitive data
    - Cloud services
- Users must authenticate using something they know (password) and an email address

Preferred Authentication Method:

- Authentication apps provide better security than SMS or email-based verification
- Authentication apps or security keys are the primary MFA method for all staff
- Primary authentication will use supplied security keys or Google Authenticator app

Additional Security Layers for IT and Systems Team:

- Conditional Access Policies: Enhanced location-based and device-based restrictions
- Privileged Access Workstations: Dedicated secure devices for administrative tasks where possible
- Time-Limited Sessions: Administrative sessions automatically expire after periods of inactivity
- Hardware Security Keys: Where technically feasible, hardware tokens (such as YubiKeys) as an additional authentication factor for critical systems

Backup Authentication Methods:

- Secondary authentication method required in case primary method is unavailable
- Backup methods will use authenticator apps
- SMS-based authentication only permitted as a last resort and must be replaced with app-based authentication within 24 hours
- All backup methods must be registered and tested before being relied upon
- Regular review of IT and Systems team access patterns and authentication logs

Compliance and Review:

- IT and Systems team members must demonstrate proper MFA configuration during six monthly access reviews
- Authentication app setup and backup method configuration is verified during annual security assessments
- Any IT and Systems team member unable to maintain enhanced MFA requirements may have administrative privileges temporarily suspended until compliance is restored
- New IT and Systems team members must complete enhanced MFA setup before being granted administrative access

Emergency Procedures:

- Emergency access procedures defined for situations where MFA systems are unavailable
- Emergency access requires approval from senior leadership and cyber_safe@spbridge.co.uk
- All emergency access activities are subject to enhanced logging and immediate post-incident review
- Temporary access must be replaced with proper MFA-protected access within 24 hours

5.3.4 Privileged Access and Account Separation

Separation of User and Administrator Accounts:

- All users must be assigned unique accounts with access limited to only the resources and data necessary for their roles (least privilege principle)
- Users must not carry out day-to-day tasks (such as email, invoicing, document creation, or web browsing) whilst logged on with administrator privileges
- Administrative privileges should only be used when performing specific administrative tasks that require elevated access
- Where users require administrative access, they must have separate accounts: one standard user account for daily work and one administrator account for privileged tasks
- Users must not share accounts or use generic/shared credentials
- Administrator accounts should not be used for internet browsing and only used for emails relating to administrative duties

Generic and External Access Accounts:

- Generic accounts providing external access (such as third-party support, vendor access, or shared service accounts) must be temporary and time-limited
- All generic external access accounts must be assigned new, unused passwords that have not been previously used
- These accounts must be disabled or deleted immediately after the authorised work is completed
- Access must be logged and monitored for the duration of use
- Generic accounts must not be used for day-to-day operations or regular business activities

5.3.5 Access Reviews and Auditing

Regular Access Reviews:

- Access rights must be reviewed based on job roles and responsibilities following the least privilege principle

- Quarterly reviews of all user access rights must be conducted by system owners in collaboration with line managers
- Reviews must verify that access levels remain appropriate for current roles and responsibilities
- Any discrepancies or unnecessary access must be removed immediately
- Documentation of all access reviews must be retained for audit purposes

Review Process:

- System owners must generate access reports showing all users and their permissions
- Line managers must confirm whether each user's access remains appropriate for their role
- HR must confirm current employment status and any role changes
- IT and Systems team must implement approved access changes within 5 working days
- Exceptions or access extensions must be documented with business justification and approved by senior management

5.4 Data Protection

- Encryption of data in transit is essential
- Comprehensive backup and recovery procedures across all systems
- Data classification and handling procedures
- Data Protection Impact Assessments (DPIAs) mandatory for all cloud suppliers and service providers
- Privacy by design principles
- Regular data retention reviews
- DPIA Requirements for Cloud Suppliers:
- Comprehensive DPIA completed before engaging any cloud service provider
- Assessment of data processing activities, risks, and mitigation measures
- Evaluation of supplier's data protection policies and technical safeguards
- Regular review and updates of DPIAs when services or risks change
- Documentation of supplier compliance with UK GDPR and data protection legislation
- Supplier details are stored and regularly reviewed in the secure Team Vault application
- Backup Infrastructure:
    - BridgeLink Systems: 24-hour automated backup cycles ensuring minimal data loss
    - Database Systems: 24-hour backup schedule with secure cloud storage
    - Google Workspace: Dual backup strategy using Google Vault for compliance and weekly external backup solution for additional protection
    - Websites: All school and group websites backed up by hosting company with regular recovery testing

    - Backup Testing: Regular restore testing to ensure backup integrity and recovery procedures

5.5 Software Licensing

- All software and cloud services used within the organisation must be properly licensed and supported:
- Only licensed software may be installed on company systems
- Unlicensed, pirated, or cracked software is strictly prohibited
- Free and open-source software (FOSS) may be used provided all licensing terms and obligations are met
- An inventory of all software licenses must be maintained and reviewed quarterly
- Cloud services must have active subscriptions and support agreements
- Unsupported or abandoned software must be replaced with supported alternatives or removed immediately
- All software procurement must be approved by IT to ensure licensing compliance

5.6 Automatic Updates

- All devices and systems within the organisation must have automatic updates enabled:
- Workstations, laptops, and mobile devices must be configured to receive and install security updates automatically
- Automatic updates must be enabled for operating systems, security software, and all applications
- Network devices (firewalls, routers, switches) should be configured for automatic firmware updates where supported by the vendor
- For systems where automatic updates cannot be enabled due to operational requirements, a documented exception must be approved by the IT Security Manager with compensating controls in place
- Users must not disable automatic updates on any company-owned or managed device
- IT will maintain a schedule for updates that require manual intervention or testing prior to deployment
- Cloud services and SaaS applications should be configured to receive automatic security updates where available
- Automatic update settings must be monitored and enforced through endpoint management tools to ensure compliance
- Where automatic updates are not permitted, business managers or a nominated member of staff must be assigned responsibility for implementing manual updates across the full estate of hardware that requires the updates. This individual must have the technical capability, access rights, and allocated time to ensure all updates are applied within the required timeframes

5.7 Unsupported Software Removal

- All software that is no longer supported by the vendor and no longer receives security updates or vulnerability fixes must be removed from devices:
- This includes operating systems, web browsers, plugins, and all application software
- IT must maintain an inventory of installed software and track vendor support status
- When software reaches end-of-life (EOL), it must be uninstalled or upgraded to a supported version within 30 days
- If unsupported software is required for critical business operations, a documented risk assessment and compensating controls must be approved by senior management
- Regular audits must be conducted to identify and remove unsupported software from all devices
- Network Segregation for Unsupported Software:
    - Where there is a documented business need to use unsupported software, the devices running this software must be moved out of scope through network segregation:
    - Devices with unsupported software must be placed on a segregated sub-set of the network with no internet access
    - This sub-set must be separated from the rest of the organisation's network by a firewall or VLAN
    - If the segregated sub-set requires internet access, the organisation will not achieve whole company certification and an excluding statement will be required
    - All segregated environments must be documented, including the business justification, devices involved, network architecture, and compensating controls in place
    - Where no unsupported software is used across the entire organisation, this must be formally documented and declared

5.8 Automated Leavers Management and Access Termination

Leavers Form Process:

- All staff departures must be processed through the mandatory automated leavers form system to ensure the security and integrity of school group systems and data.
- Mandatory Process Requirements:
    - The leavers form must be completed for every staff member departure, regardless of role or reason for leaving
    - Form completion is required for all students, permanent staff, temporary staff, contractors, and volunteers
    - The form must be submitted immediately upon notification of departure or as soon as the departure date is confirmed
    - No exceptions to this process are permitted - all leavers must be processed through this system
- Automated Access Termination:
    - System Integration:
    - The leavers form is directly integrated with all IT systems and access control mechanisms

    - Upon form completion and approval, automated termination processes are triggered
    - All access rights are automatically scheduled for termination on the specified departure date
    - The system operates on the principle of "secure by default" - all access is removed unless specifically exempted
- Termination Scope:
    - The automated system will terminate access using Spaghetti Bridge credentials to:
        - All network accounts and login credentials
        - Email systems and communication platforms
        - All access to Bridge Link
        - Educational platforms and learning management systems
        - Administrative and financial systems
        - Building access cards and security systems
        - VPN and remote access capabilities
        - Cloud services and applications (Google Workspace, etc.)
        - Any system-specific applications or databases

Timing and Execution:

- Access termination occurs automatically at 23:59 on the departure date specified in the leavers form
- Critical systems may have access terminated earlier in the day if specified in the form
- Emergency termination can be triggered immediately if required for security purposes
- System owners are automatically notified of pending terminations 48 hours in advance
- Automated Notifications:
    - The leavers form system automatically generates notifications to:
    - Relevant system administrators (48 hours before termination)
    - Line managers (confirmation of completed termination)
    - HR department (audit trail and record keeping)
- Stakeholder Communication:
    - All relevant departments are notified through the automated system
- Special access requirements or delayed terminations must be documented and approved
- Any system access that needs to continue beyond the departure date requires senior management approval
- Communication includes details of what access has been terminated and when
- Mandatory Compliance:
    - Use of the leavers form system is mandatory and non-negotiable for all staff departures
    - Failure to use the system represents a significant security risk and policy violation
    - Any staff departure not processed through the system must be reported to cyber_safe@spbridge.co.uk immediately

    - Regular audits will be conducted to ensure 100% compliance with this process

Data Protection:

- All data associated with terminated accounts is handled according to data retention policies
- Personal data is processed lawfully and retained only as long as necessary
- Former staff members' data in systems is reviewed and archived appropriately
- GDPR compliance is maintained throughout the leavers process

Emergency and Exception Procedures:

- Emergency Termination:
    - In cases of immediate termination or security incidents, access can be terminated instantly
    - Emergency termination overrides the standard automated schedule
    - Post-incident review is required for all emergency terminations
- Approved Exceptions:
    - Any request to maintain access beyond the departure date requires written approval from senior management
    - Exceptions must specify exactly which systems need continued access and for how long
    - All exceptions are subject to enhanced monitoring and regular review
    - Temporary access for knowledge transfer or project completion must have defined end dates
- Audit and Review Requirements:
    - Regular Auditing:
        - Monthly audits of all processed leavers forms and access terminations
        - Quarterly review of the automated system's effectiveness and compliance rates
        - Annual assessment of the leavers management process and policy effectiveness
        - Independent verification that no unauthorised access remains active
- Documentation and Records:
    - Complete audit trail maintained for all leavers processing
    - Records include form completion dates, approval workflows, and termination confirmations
    - Documentation retained in accordance with legal and regulatory requirements
    - Regular backup of leavers system data and audit logs
- Continuous Improvement:
    - Regular review of the leavers process based on audit findings and security assessments
    - Updates to the automated system to address identified gaps or improvements
    - Staff feedback collection to improve the efficiency and effectiveness of the process

- Integration of lessons learned from security incidents involving former staff access

6. Incident Management

6.1 Incident Classification

- **Category 1 - Critical:** Incidents affecting multiple schools, significant data breaches, ransomware, or complete system outages
- **Category 2 - High:** Incidents affecting individual schools, suspected data breaches, or major system compromises
- **Category 3 - Medium:** Minor security violations, phishing attempts, or localised system issues
- **Category 4 - Low:** Policy violations, failed login attempts, or awareness issues

6.2 Reporting Procedures

School-Level Reporting:

- Any suspected cyber security incident must be reported immediately to any member of the School Senior Leadership Team (SLT)
- SLT member receives the initial report and assesses the severity
- SLT makes the decision on whether to escalate to the Cyber Safe team
- For Category 1 and 2 incidents, SLT must notify cyber_safe@spbridge.co.uk within 1 hour of becoming aware
- For Category 3 incidents, SLT must notify cyber_safe@spbridge.co.uk within 4 hours
- Category 4 incidents may be reported during normal business hours but within 24 hours

Direct Reporting Routes:

- Staff may report directly to cyber_safe@spbridge.co.uk for urgent incidents
- Anonymous reporting available through designated secure channels
- Emergency contact procedures for out-of-hours incidents

6.3 Cyber Safe Team Response and Escalation

Initial Response (cyber_safe@spbridge.co.uk):

- Immediate acknowledgment of all incident reports
- Initial assessment and classification of incidents
- Activation of appropriate response procedures
- Coordination with affected schools and departments

Response Activities:

- Incident containment and damage limitation
- Forensic investigation where appropriate
- Communication with affected parties following communication plan
- Remediation and system recovery
- Evidence preservation for potential legal action

External Escalation Procedures:

The Cyber Safe team will escalate to external authorities within industry standard timeframes:

- **Data Protection Authority (ICO):** Within 72 hours for personal data breaches
- **National Cyber Security Centre (NCSC):** For significant incidents affecting critical systems
- **Law Enforcement:** For criminal activity including fraud, ransomware, or targeted attacks
- **Department for Education:** For incidents affecting educational operations or student safety
- **Cyber Security Insurance Provider:** Within 24 hours for covered incidents
- Upon invocation, the Business Continuity Plan takes precedence, with cyber response activities coordinated under the Spaghetti Bridge crisis management framework.

Contact Details

National Cyber Security Centre (NCSC)

- Report incidents: https://www.ncsc.gov.uk/report-an-incident
- Phone: 0300 303 5222
- Email: report@ncsc.gov.uk

Action Fraud (UK's national reporting centre for fraud and cybercrime)

- Report online: https://www.actionfraud.police.uk
- Phone: 0300 123 2040

Police - for emergencies or ongoing crimes

- Emergency: 999
- Non-emergency: 101

Information Commissioner's Office (ICO)

- Data breach reporting: https://ico.org.uk/for-organisations/report-a-breach/
- Phone: 0303 123 1113
- Email: casework@ico.org.uk

- Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Communication and Updates:

- Regular updates to affected schools and senior leadership
- Status reports at defined intervals until incident resolution
- Post-incident communication to all stakeholders
- Lessons learned documentation and policy updates

6.4 Incident Response Tools and Resources

The Cyber Safe team maintains access to:

- Incident tracking and case management systems
- Forensic analysis tools and external specialist support
- Legal and regulatory notification templates
- Vendor and supplier escalation contacts

6.5 Post-Incident Activities

- Comprehensive incident review and lessons learned
- Policy and procedure updates based on findings
- Additional training where gaps are identified
- Insurance claims processing where applicable
- Legal action coordination if required

7. Training and Awareness

7.1 Staff Training

- Annual cyber security training for all staff
- Role-specific training based on access levels
- Regular updates on emerging threats
- Simulated phishing exercises
- Incident response training for key personnel
- Termly training and review on cyber security training for members of the IT and Systems Team
- Any individual that is moved into a new role may require new access, the IT and Systems team must be notified before the new role is started so that access control is established for the new role and removed from the old role.

7.2 Student Education

- Age-appropriate digital citizenship curriculum
- Online safety education
- Regular assemblies and awareness sessions
- Peer education programs
- Integration with PSHE and computing curricula

7.3 Ongoing Awareness

- Regular security bulletins and updates
- Poster campaigns and visual reminders
- Recognition programs for good security practices
- Integration of security awareness into staff meetings
- Phishing simulations

8. Compliance and Monitoring

8.1 Regular Assessments

- Annual cyber security risk assessments
- Annual penetration testing conducted by qualified external security companies using manual, hands-on testing methodologies
- Quarterly policy compliance reviews
- Technical security testing and vulnerability assessments
- Third-party security audits where appropriate

8.2 Key Performance Indicators

- Number of security incidents by category
- Time to detect and respond to incidents
- Training completion rates
- Compliance assessment scores
- System availability and performance metrics
- Backup success rates and recovery testing results
- Mean time to recovery (MTTR) for system outages

9. Policy Enforcement

9.1 Disciplinary Measures

Violations of this policy may result in disciplinary action appropriate to the severity of the breach and the user's role within the school group and in line with the group's normal HR guidelines.

9.2 Legal Action

Serious violations may result in referral to law enforcement agencies and civil or criminal prosecution under relevant UK legislation.

10. Business Continuity

10.1 Backup and Recovery

Spaghetti Bridge Ltd maintains comprehensive backup solutions to ensure business continuity and data protection:

System-Specific Backup Schedules:

- **BridgeLink Systems:** Automated 24-hour backup cycles with incremental daily backups and full weekly backups
- **Database Infrastructure:** 24-hour backup schedule with transaction log backups every 15 minutes for minimal data loss
- **Google Workspace (Email, Drive, etc.):**
    - Primary: Google Vault for compliance, litigation hold, and data retention
    - Secondary: Weekly external backup solution providing additional protection and granular recovery options
- **School and Group Websites:** Automated backups managed by hosting company with daily incremental and weekly full backups

Backup Security and Storage:

- All backups encrypted both in transit and at rest
- Geographic separation of backup storage locations
- Regular integrity checks and corruption detection
- Secure access controls for backup systems
- Documented retention periods aligned with legal and regulatory requirements

Recovery Procedures:

- Regular testing of backup restoration processes will take place each school term on all systems by using restoration testing
- Documented recovery time objectives (RTO) and recovery point objectives (RPO) for each system
- Prioritised recovery sequence for critical systems
- Communication procedures during recovery operations
- Staff training on backup and recovery procedures

10.2 Remote Working

- Secure VPN access for authorised remote work where the work is not being carried out on a cloud system
- Device security requirements for home working
- Data handling procedures for remote access

11. Policy Review and Updates

This policy will be reviewed annually or following significant security incidents, technological changes, or regulatory updates. All stakeholders will be consulted during policy reviews, and updated versions will be communicated across the school group.

12. Contact Information

- **IT Support:** it_admin@spbridge.co.uk
- **Emergency IT Issues:** cyber_safe@spbridge.co.uk

13. Domain Name Security

All organisational domain names must be secured and managed in accordance with the following requirements:

Registration and Ownership

- Domain names must be registered under the organisation's legal name with accurate contact details maintained at all times
- A central register of all owned domains must be maintained by the IT & Systems team
- Domain registrations must be renewed at least 30 days before expiry, with auto-renewal enabled where possible
- DMARC records are in place for all domain names

Access Control

- Registrar account access must be restricted to authorised IT and System Administrators only
- Strong, unique passwords must be used for all registrar accounts
- Multi-factor authentication (MFA) must be enabled on all domain registrar accounts

- Access credentials must be stored securely in Zoho Vault

Technical Security

- Domain locking must be enabled to prevent unauthorised transfers
- WHOIS privacy protection should be enabled where appropriate
- DNSSEC (Domain Name System Security Extensions) should be implemented where supported
- Regular audits of DNS records must be conducted to detect unauthorised changes

Monitoring and Alerts

- Automated alerts must be configured for domain expiry warnings, DNS changes, and unauthorised access attempts
- Regular checks for typosquatting or similar fraudulent domains must be conducted

Transfer and Changes

- Any domain transfers or significant DNS changes require approval from the Group Head of IT and Systems
- A change log must be maintained for all domain-related modifications

For further advice and support regarding this policy please contact the Group Head of IT and Systems.

14. Ransomware Response

Policy Statement

Spaghetti Bridge Ltd does not support or condone the payment of ransoms to cybercriminals. This policy establishes our approach to ransomware incidents and ransom demands.

Core Principles

- The organisation's default position is to **not pay ransoms** under any circumstances
- Paying ransoms funds criminal enterprises, encourages further attacks, and provides no guarantee of data recovery
- Recovery will be prioritised through backup restoration and legitimate recovery methods
- All ransomware incidents will be treated as Category 1 (Critical) incidents

Immediate Response to Ransomware

Upon detection of ransomware:

1. Immediately isolate affected systems from the network
2. Do not shut down infected systems (this may hinder forensic investigation)
3. Notify cyber_safe@spbridge.co.uk immediately
4. Preserve all evidence including ransom notes, payment demands, and communication channels
5. Do not communicate with threat actors without authorisation from the Cyber Safe team

Assessment and Decision Making

The Cyber Safe team will:

- Assess the extent of the infection and data compromise
- Evaluate backup availability and recovery feasibility
- Determine impact on critical educational services and student safety
- Engage with law enforcement (Action Fraud, National Crime Agency)
- Consult with the National Cyber Security Centre (NCSC)
- Contact our cyber insurance provider within 24 hours
- Brief senior leadership on recovery options and timelines

Communication with Threat Actors

- Only the Cyber Safe team, in consultation with law enforcement and legal counsel, may communicate with threat actors
- All communications must be documented and shared with law enforcement
- Communication is solely for intelligence gathering and does not imply willingness to pay
- No commitments or agreements may be made without CEO approval

Ransom Payment Considerations

Payment of ransom may only be considered in exceptional circumstances where **all** of the following conditions are met:

- Student safety or safeguarding is at immediate risk
- Critical systems cannot be recovered through any other means
- Recovery time would cause unacceptable harm to students or operations
- Law enforcement has been consulted and their guidance considered
- Legal counsel has been consulted
- Cyber insurance provider has been consulted
- The decision has been approved by the CEO and Board Chair

Even where these conditions are met, payment remains a last resort option only.

Payment Authorisation

If payment is authorised as a last resort:

- Payment must be authorised in writing by both the CEO and Board Chair
- All payments must comply with UK legal requirements and sanctions regulations
- Law enforcement must be notified before and after any payment
- Payment must be facilitated through specialist incident response firms
- All transaction details must be documented for legal and insurance purposes
- No guarantee of data recovery should be assumed

Alternative Recovery Actions

Priority will be given to:

- Restoration from secure backups (primary recovery method)
- Engagement of specialist cyber incident response and forensic companies
- Cooperation with law enforcement and NCSC
- Use of legitimate decryption tools where available
- Rebuilding systems from clean images if necessary

Post-Incident Requirements

Following any ransomware incident:

- Comprehensive investigation into root cause and attack vector
- Review and testing of all backup and recovery procedures
- Enhanced security controls implementation
- Staff training on lessons learned
- Updates to this policy based on incident findings
- Notification to ICO if personal data was compromised
- Communication to affected parties as required by GDPR

Legal and Regulatory Compliance

- All actions must comply with UK law including sanctions regulations
- ICO must be notified within 72 hours if personal data is compromised
- Department for Education must be notified of significant incidents
- Insurance claims must be filed in accordance with policy terms
- Law enforcement cooperation is mandatory throughout

Staff Training

All staff will receive training on:

- Recognising ransomware indicators
- Immediate actions if ransomware is suspected
- The organisation's no-payment policy stance
- Prevention measures and good cyber hygiene practices

Signable

Issuer	Spaghetti Bridge Ltd
Document generated	Mon, 22nd Jun 2026 10:20:49 BST
Document fingerprint	9fda23f5b21668c101e115d4f59313fc

Parties involved with this document

Document processed	Party + Fingerprint
Mon, 22nd Jun 2026 11:08:10 BST	Stephen Bradshaw - Signer (717e70b8017a1b462437d1a4b9cea276)
Thu, 25th Jun 2026 9:39:43 BST	Dan Alipaz - Signer (78b33cfb7338bb174ea834832b494249)

Audit history log

Date	Action
Mon, 22nd Jun 2026 10:20:49 BST	Envelope generated by Amy Fielding (193.223.70.0)
Mon, 22nd Jun 2026 10:20:50 BST	Document generated with fingerprint 9fda23f5b21668c101e115d4f59313fc (193.223.70.0)
Mon, 22nd Jun 2026 10:22:14 BST	Sent the envelope to Stephen Bradshaw (stephen.bradshaw@spbridge.co.uk) for signing (193.223.70.0)
Mon, 22nd Jun 2026 10:22:14 BST	Sent the envelope to Dan Alipaz (dan.alipaz@spbridge.co.uk) for signing (193.223.70.0)
Mon, 22nd Jun 2026 10:22:14 BST	Document emailed to dan.alipaz@spbridge.co.uk
Mon, 22nd Jun 2026 10:22:15 BST	Document emailed to stephen.bradshaw@spbridge.co.uk
Mon, 22nd Jun 2026 10:22:17 BST	Dan Alipaz opened the document email. (74.125.150.7)
Mon, 22nd Jun 2026 10:22:18 BST	Stephen Bradshaw opened the document email. (74.125.150.7)
Mon, 22nd Jun 2026 10:22:23 BST	Dan Alipaz opened the document email. (66.249.93.38)
Mon, 22nd Jun 2026 10:23:52 BST	Stephen Bradshaw opened the document email. (66.249.93.33)
Mon, 22nd Jun 2026 11:07:44 BST	Stephen Bradshaw opened the document email. (66.249.93.39)
Mon, 22nd Jun 2026 11:07:50 BST	Stephen Bradshaw viewed the envelope (185.66.206.162)
Mon, 22nd Jun 2026 11:07:57 BST	Stephen Bradshaw viewed the envelope (82.15.95.138)
Mon, 22nd Jun 2026 11:08:10 BST	Stephen Bradshaw signed the envelope (185.66.206.162)
Mon, 22nd Jun 2026 12:57:10 BST	Dan Alipaz opened the document email. (66.249.93.41)
Thu, 25th Jun 2026 8:56:18 BST	Sent Dan Alipaz a reminder to sign the document. (141.195.137.67)
Thu, 25th Jun 2026 8:56:18 BST	Document emailed to dan.alipaz@spbridge.co.uk
Thu, 25th Jun 2026 8:56:21 BST	Dan Alipaz opened the document email. (74.125.150.7)
Thu, 25th Jun 2026 9:39:29 BST	Dan Alipaz opened the document email. (66.249.93.36)

Thu, 25th Jun 2026 9:39:33 BST	Dan Alipaz viewed the envelope (86.152.236.64)
Thu, 25th Jun 2026 9:39:41 BST	Dan Alipaz viewed the envelope (82.15.95.134)
Thu, 25th Jun 2026 9:39:43 BST	Dan Alipaz signed the envelope (86.152.236.64)
Thu, 25th Jun 2026 9:39:43 BST	This envelope has been signed by all parties (86.152.236.64)
Thu, 25th Jun 2026 9:39:43 BST	Signed document confirmation emailed to stephen.bradshaw@spbridge.co.uk (86.152.236.64)
Thu, 25th Jun 2026 9:39:43 BST	Signed document confirmation emailed to dan.alipaz@spbridge.co.uk (86.152.236.64)