Access Control Policy

Version 1.02 – Jan 2020

Owner: Ms Sophie Allen - Headteacher

Review Date: Jan 2020

Version control table

Version Number	Date	Purpose/Change	Reviewer / Authoriser
1.0	22/05/2018	Policy created	Veren Vaja on behalf of The Stonebridge School
1.01	23/05/2018	School specific changes	Veren Vaja on behalf The Stonebridge School
1.02	23/01/2020	Read through for relevance	Veren Vaja on behalf The Stonebridge School

Contents

1 About this document

To define the requirements of The Stonebridge School to ensure that access to information assets is authorised and subject to identification and authentication controls.
To establish the requirements for controlling access to The Stonebridge Schools information or information that it is responsible for, including computing and physical resources.
Computer systems, networks and allied hardware and other peripherals are an integral part of our operations and represent substantial investment. It is the purpose of the Access Control Policy to ensure that all access to information assets is properly authorised, maintained and reviewed.

2 Scope

This Access Control Policy shall apply to all access to The Stonebridge School's information assets. All Users provided with access to The Stonebridge School's information systems shall comply with this Access Control Policy as indicated in the IT Acceptable Use Policy (AUP). Access to physical and non-physical assets will be governed under the same principles. This Access Control Policy shall establish the Logical and Physical Access control requirements for protecting the entire university's information systems and hardcopy data.

3 Policy statement

- The Stonebridge School, located at Shakespeare Avenue, Stonebridge, London, NW10 8NG & The Stonebridge Annexe at Twybridge Way, Stonebridge, London, NW10 0ST, are committed to compliance with all UK laws in respect of personal data, the protection of the “rights and freedoms” of individuals whose information is collected and processed in accordance with the General Data Protection Regulation (GDPR), and the UK Data Protection Act 2018.
- This policy should be read in conjunction with The Stonebridge School’s IT Acceptable Use Policy, which summarises what The Stonebridge Schools deems to be acceptable use of information systems
- It is the responsibility of every User with access to the School's information systems to ensure that they have read and understood this document. All Users are obliged to adhere to this policy. Any deliberate or informed breach of this Policy may lead to disciplinary action up to and including dismissal from the university in accordance with the Acceptable Use Policy.
- The Stonebridge School’s information systems are provided for business purposes only and this Access Control Policy is used to ensure that Users:
    - Comply fully with current legislation;
    - Comply with other relevant The Stonebridge Schools policies.
    - Do not introduce unnecessary risk to The Stonebridge School.
- Access allocation shall be monitored to ensure compliance with this Access Control Policy.

- All Users, who use the School's information assets and information systems, shall be responsible for safeguarding those resources and the information the information Owners hold, from disruption or destruction.
- The Access Control Policy shall apply to all Users who have access to the School's information assets, including remote access.
- Failure to comply may result in the offending employee being subject to disciplinary action up to and including termination of employment.
- The use of the school's information assets and information systems indicates acceptance of this Access Control Policy.

4 Implementation Responsibilities

- The Stonebridge Schools IT Services shall ensure that Users are provided with education and training to ensure compliance with this Access Control Policy.
- The Stonebridge Schools IT Services shall develop, maintain and publish standards, processes, procedures and guidelines to achieve compliance with this Access Control Policy.
- Annually review the Access Control processes, standards and procedures, to achieve compliance with this Access Control Policy and shall support the Access Control Strategy and provide security specific input and guidance where required.
- IT asset owners and authorised users shall be assigned for each identified IT asset in order to approve or reject requests for access to their system.
- IT asset owners and authorised users shall check the validity of all user access requests to information assets owned by them before implementation.
- IT asset owners and authorised users shall authorise employees requiring access to information assets owned by them.
- The School Business manager shall inform the IT department of users starting, moving and leaving the Schools Employment.
- All appropriate line managers shall authorise any requirement to changes to user's access rights on the information systems.
- Users shall not share access codes and/or passwords, if access to other information systems are required then a formal request shall be put forward for authorisation by an appropriate line manager.
- Users shall not share their physical access cards; if physical access to restricted areas is required then a formal request shall be put forward for authorisation by the line manager.
- Users shall be responsible for the security (and secrecy) of their own secret authentication information. In no circumstances is secret authentication information to be shared.
- The School shall be responsible for ensuring all Users of The Stonebridge School’s information systems read and acknowledge the policy principles extracted from this Access Control Policy and included in the Acceptable Use Policy.

5 The Access Control Principles

- All information assets shall be "owned" by a named individual within The Stonebridge School.
- A process for user access requests, which mandates the steps to be taken when creating or modifying user access shall be defined, documented, annually reviewed and updated. The scope of this process must include network, application and database access and be applicable to any third party access.
- Access to information assets shall be restricted to authorised employees and shall be protected by appropriate physical and logical authentication and authorisation controls.
- Users shall be authenticated to information systems using accounts and passwords.
- Users are required to satisfy the necessary personal security criteria, before they can be authorised to access information assets of a corresponding classification.
- Users who have satisfied all necessary criteria may be granted access to information assets only on the basis that they have a specific need to know, or to "have-access-to", those information assets.
- The classification of an information asset does not, in itself, define who is entitled to have access to that information. Access is further filtered by any applicable privacy restrictions as dictated by other The Stonebridge School Policies (such as the Data Protection Policy)
- Access privileges shall be authorised by the appropriate information Owner and allocated to employee, based on the minimum privileges required to fulfil their job function.
- Administrator accounts shall only be granted to those users who require such access to perform their job function. Administrator accounts shall be strictly controlled and their use shall be logged, monitored and regularly reviewed.
- Users with administrator access shall only access sensitive data if so required in the performance of a specific task.
- Users with administrator access shall also have an unprivileged account, which shall be used for all purposes not requiring administrator access, including but not limited to electronic mail.
- Line managers, information asset owners and authorised users shall ensure rights and privileges granted to Users of information assets are reviewed on at least every 6 months to ensure that they remain appropriate and to compare user functions with recorded accountability.
- Access shall be granted only to those systems or roles that are necessary for the job function of the user.
- Detailed processes shall be developed and followed for terminating, modifying or revoking an employee's access, as part of the Movers/Leavers process.
- In certain instances, particular access may be required for emergency reasons, such as undertaking emergency system maintenance. Requests for emergency access shall be directed to The Stonebridge School's Chief Information Officer, and shall be approved by the information asset owner or authorised user. Requests and approval should be documented, if possible, before the change is required stipulating an expiry period, which shall be enforced, for the access rights. A request for change shall be documented retrospectively where it is not possible to do this in advance.

- All third party access (Contractors, Business Partners, Consultants, Vendors) shall be authorised by an appropriate information Owner and, if necessary, monitored.
- Remote access to The Stonebridge School's networks shall be appropriately authorised on a least privilege basis, with access only granted to systems and resources where there is an explicit business requirement. Only employees of the School or authorised third parties shall be able to connect to the Schools network infrastructure remotely.
- Only authorised personnel shall be given access to secure areas at the school's premises and any third party premises where sensitive information is processed or maintained, or physical assets are held.
- All access to areas hosting systems that store, process, or transmit sensitive data (e.g. datacentres) shall be controlled, monitored by cameras and logged. Logs shall be regularly audited, correlated with other logs and securely stored for at least three months, unless otherwise restricted by law.
- All visitors shall have authorisation prior to entering any of the university's sites where sensitive data is processed or maintained.
- All visits shall be logged and details of logs retained for a minimum of one month, unless otherwise restricted by law. Reception staff shall be made aware of their responsibility to log every visitor to The Stonebridge School sites.
- Employees shall challenge and/or report any visitors found unsupervised or acting suspiciously at any site where sensitive The Stonebridge School data is processed or maintained.
- Site management shall perform a formal review of physical access rights at least every 6 months to identify unauthorised or expired access. Access controls shall be revoked in instances where access is no longer necessary for job function.

6 Responsibilities

Members of The Stonebridge School:

All members of The Stonebridge School, The Stonebridge School associates, and agency staff working for The Stonebridge School may have or require access to The Stonebridge School's data or IT systems, and may be responsible for the systems upon which The Stonebridge School data reside.

System Owners

Those with responsibility for systems (including designating access) upon which The Stonebridge School data reside. This includes but is not limited to teachers, learning assistants and support staff.

ICT Network Manager

Responsible for:

• administering access to The Stonebridge School's Active Directory environment and many of its systems

• implementing role based access control upon the School's shared access file systems,

• creating The Stonebridge School's Active Directory user accounts and passwords

• maintaining The Stonebridge School's network infrastructure, firewalls and network zoning

• maintaining the External Collaborators Access

• Responsible for writing this policy and establishing access control principles.

• investigating breaches and recommending remedial actions

• organising annual penetration tests

• Administration of door access control systems

• Cancelling Staff, Contractor ID cards

Site Staff

Responsible for:

• Physical security on School Site(s)

• Security of comms rooms and onsite datacentre

HeadTeacher

Responsible for approving information security policies.