Sophia
HIGH SCHOOL

ACCESS CONTROL POLICY

2025 - 2026

Review Interval	Reviewed	Next Review start
3 years	Nov 2022	July 2025

Version History

Version	Date	Approved by	Notes
1.13	2 Nov 2018	MM	
1.14	1st Sept 2022	MM	
1.15	8th August 2023	MM	
1.16	30th July 2025	AI	

Contacts

Position	Name	Email	Notes
Head of Technology and Development	Alberto Iglesias	alberto.iglesias@sophia.app	there are specific items that are not of interest to the user, like IIS, Apache , Database access, etc

Communications & Training

Will this document be publicised through internal communications?	No
Will training needs arise from this policy?	No
If yes, please give details	

ACCESS CONTROL POLICY

Sophia Technologies Ltd and Sophia High School Ltd, implements physical and logical access controls across its networks, IT systems and services in order to provide authorised, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability in accordance with the Information Security Policy.

Access control systems are in place to protect the interests of all authorised users of Sophia IT systems, as well as data provided by third parties, by creating a safe, secure and accessible environment in which to work.

The School was first approved with Cyber Essentials in October 2021 with a successful renewal on 19th April 2023. Certificate Number 88cfd58d-1951-418e-9a8e-18870aedf1a9

1.1. Scope

This policy covers all Sophia networks, IT systems, data and authorised users.

1.2. Out of Scope

The Sophia external website and other information classified a ‘Public’. Systems outside IMT control will not fall under Sections 2.2.1 and 2.2.2.

Privileged access to non-IMT controlled systems, resources and applications is the responsibility of the system, resource or application owner, not IMT. The authorisation and auditing processes involved in granting access to these resources is the responsibility of the resource owners.

2. Policy

2.1. Principles

Sophia will provide all employees, students and contracted third parties with access to the information they need to carry out their responsibilities in as effective and efficient manner as possible.

2.1.1. Generic identities

Generic or group IDs shall not normally be permitted as means of access to Sophia data, but may be granted under exceptional circumstances if sufficient other controls on access are in place.

Under all circumstances, users of accounts must be identifiable in order for Sophia to meet the conditions for our Digital Learning Environment, Google for Education Workspace and Athena Digital Education Platform (as laid out in the ‘Acceptable Use Policy’).

Generic identities will never be used to access Confidential Data or Personally Identifiable Information.

2.1.2. Privileged accounts

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled and not provided by default.

Authorisation for the use of such accounts shall only be provided explicitly, upon written request from the Directors / Co-Founders, and will be documented by the system owner.

Technical teams shall guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and / or integrity.

Privileged accounts must not be used for standard activities; they are for program installation and system reconfiguration, not for program use, unless it is otherwise impossible to operate the program.

2.1.3. Least privilege and need to know

Access rights to both physical and logical assets will be accorded following the principles of least privilege and need to know.

2.1.4. Maintaining data security levels

Every user must understand the sensitivity of their data and treat them accordingly. Even if technical security mechanisms fail or are absent, every user must still maintain the security of data commensurate to their sensitivity.

Users electing to place information on non-managed systems and databases, digital media, cloud storage, or removable storage devices are advised by our Technology Department only do so where:

- such an action is in accord with the information’s security classification
- the provision meets any research data supplier or other contracts,
- other protective measures (such as the use of encryption) have been implemented.

Users are consequently responsible in such situations for ensuring that appropriate access to the data is maintained in accordance with the Information Security Policy and any other contractual obligations from data providers they may have to meet.

Users are obligated to report instances of non-compliance to the Head of Technology via Alberto Iglesias: alberto.iglesias@sophia.app

2.2. Access Control Authorisation

2.2.1. User accounts

Access to Sophia IT resources and services will be given through the provision of a unique user account and complex password.

Accounts are provided on the basis of valid records in the HR and student information systems. For any user not in either of those systems, access is granted via the appropriate staff or associate form signed by a Head of Department or Departmental manager. Default access is granted only to Google Classroom, a personal Google Drive and an email account.

2.2.2. Passwords

Password issuing, strength requirements, changing and control will be managed through formal processes.

Password issuing will be managed by the IT Service Desk for staff and IT Helpdesk for students.

Password changing can be performed via the Google for Education Workspace Administrator account or follow a request made to our Technology Team via an identifiable email.

2.2.3. Access to Confidential, Restricted and Internal Use information

Access to ‘Confidential’, ‘Restricted’ and ‘Internal Use’ information will be limited to authorised persons whose job or study responsibilities require it, as determined by law, contractual agreement with interested parties (e.g. DfE, CIS, Ofsted and other research data providers) or the Privacy Policy.

Access to any of these resources will be restricted by use of firewalls, network segregation, secure log-on procedures, access control list restrictions and other controls as appropriate.

The responsibility to implement access restrictions lies with the data processors and data controllers, but must be implemented in line with this policy.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within Sophia’s Active Directory domains and administered by our Technology Team

There are no restrictions on the access to ‘Public’ information.

2.2.4. Policies and guidelines for use of accounts

Users are expected to become familiar with and abide by Sophia, standards and guidelines for appropriate and acceptable usage of the networks and systems. This includes the Digital Safety Policy, Acceptable Use Policy and Online Safeguarding Policies.

2.2.5. Access for remote users

Access for remote users shall be subject to authorization by Technology Team and be provided in accordance with the Online Safeguarding Policy, Digital Safety Policy and Acceptable Use Policy. No uncontrolled external access shall be permitted to any network device or networked system.

2.2.5a Use of VPN to access the SHS platform, including live and recorded lessons:

To ensure the safety and security of our students and staff, and to maintain the integrity of our online learning environment, we strictly prohibit the use of Virtual Private Networks (VPNs) when accessing school-owned email accounts and our online learning platform.

The use of VPNs poses significant risks to our unique remote learning environment, including:

- Circumventing school and google workspace web filters and content control measures, potentially exposing students to harmful or inappropriate material.
- Concealing user activity, making it difficult for the school to monitor and detect potential safeguarding risks or unauthorised access.
- Enabling unregulated direct communication from anywhere, which may lead to student vulnerabilities and compromise the school's ability to fulfil its duty of care.
- Increasing the risk of ransomware attacks and other cyber threats, which can jeopardise the security and integrity of the school's network and student data.
- Compromising data security as VPNs can create additional entry points into the school's network, potentially compromising the security of sensitive student data and intellectual property
- Interfering with google workspace performance: The use of VPNs can strain the school's google workspace network resources and slow down internet speeds, negatively impacting the quality of the online learning experience for all students.

As part of our commitment to meeting the DfE's filtering and monitoring standards, Sophia High School employs a range of strategies to minimise safeguarding risks on internet-connected devices, including:

- Physical monitoring by staff watching user screens in online lessons
- Live supervision by staff using device management software in lessons
- Network monitoring using log files of internet traffic and web access
- Annual review of access control, security and online safeguarding or more frequently if risks are identified.

Our filtering systems are designed to identify device names or IDs, IP addresses, and, where possible, individual users, along with the time and date of attempted access and any blocked search terms or content.

The senior leadership team is responsible for procuring, documenting, reviewing, and overseeing these systems to ensure their effectiveness in meeting our statutory requirements under KCSIE and the Prevent duty.

We recognise that effective filtering and monitoring should not unreasonably impact teaching and learning or school administration, nor should it restrict students from learning how to assess and manage risk themselves.

As such, we conduct regular reviews of our systems, at minimum annually, or when a safeguarding risk is identified, there is a change in working practise, or new technology is introduced.

By prohibiting the use of VPNs, we aim to maintain a transparent, secure, and accountable online learning environment that allows us to effectively monitor and mitigate potential risks. We appreciate the cooperation of our students and their families in adhering to this policy, as it is essential to ensuring the safety and well-being of our entire school community.

Parents and guardians are required to acknowledge and agree to this VPN prohibition as part of the terms and conditions for enrolling their child at Sophia High School.

Any violation of this policy may result in disciplinary action, up to and including restriction of access to the online learning platform and school email accounts and/or termination of the student's enrolment.

2.2.6. Physical access control

Physical access at Sophia Head Office, where restricted, is controlled primarily via Sophia Access Codes.

2.2.6.1. Lost cards

Lost Sophia Access Cards must immediately be reported to the Head of Technology and Business Management Office. The Business Management Office will cancel the card through the physical access control system.

2.2.6.2. Reissuing cards

Replacement cards cannot be issued until the Security Office has confirmed that a prior card has been cancelled.

2.3. Access Control Methods

Access to data is variously and appropriately controlled according to the data classification levels.

Access control methods used by default include:

- explicit logon to devices,
- Google Workspace share and file permissions to files and folders,
- user account privilege limitations,
- server and workstation access rights,
- firewall permissions,
- network zone and VLAN ACLs,
- IIS/Apache intranet/extranet authentication rights,
- Sophia user login rights,
- Database access rights and ACLs,
- Encryption at rest and in flight
- Any other methods as contractually required by interested parties.

Access control applies to all Sophia-owned networks, servers, workstations, laptops, mobile devices and services run on behalf of Sophia.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within Sophia’s Active Directory domains.

2.4. Cloud Systems

The use of cloud-based systems by Sophia must in all respects meet the access control provisions laid out in this policy.

Evaluation of access controls implemented in any cloud system is performed during the vendor assessment and implementation stages of any project.

All completed cloud questionnaires are assessed by the Technology Team with appropriate remedial actions recommended or risks to be accepted before use is authorised. Where risks are deemed too large for the Technology Team, the project will be referred to Directors for approval.

Cloud systems must meet Sophia’s Minimum Standards for Cloud systems.

2.5. Penetration Tests

Sophia’s access control provision will be regularly made subject to penetration tests, in order to ascertain the effectiveness of existing controls and expose any weaknesses. Tests will include, where appropriate and agreed to, the systems of cloud service providers.

2.6. Further Policies, Codes of Practice, Procedures and Guidelines

This policy sits beneath Sophia’s overarching Online Safeguarding Policy, Acceptable Use and Digital Safety Policies including Privacy Policy and Cookies Policy.

Other supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on Sophia’s website. All staff, students and any third parties authorised to access Sophia’s network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

2.7. Review and Development

This policy shall be reviewed and updated regularly by the Board of Directors and the Head of Technology. We use the Cyber Essentials auditor external to our Technology team to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations. Additional regulations may be created to cover specific areas.

The Directors and Head of Technology will determine the appropriate levels of security measures applied to all new information systems.