School Spider by Iris

Information Security Assurance Statement

Document control
Version number: 1.0
Owner: Alex Ellis
Date of last update: 06/03/2025
Document type: Information Security Assurance Statement
Replaces: N/A
Approved by:
Approval date:
Data protection impact screening:
Date of next formal review:

Contents

Information security assurance statement

Objective of this document

The purpose of this information security assurance statement is to provide customers of School Spider by IRIS with transparency as to the security and personal data compliance of this product from all threats, whether internal or external, deliberate or accidental. Also, this document aims to ensure legal compliance, business continuity, minimise business damage and maximise client confidence in School Spider as a thoroughly secure software and service provider.

Description of the data processing carried out by School Spider

School Spider by Iris is a product that enables schools to easily communicate & engage with parents and also to accept payments for products created by the school.

Schools will typically link their MIS system to School Spider via the Wonde middleware. This then gives us access to the data that we need in order to communicate and engage with parents, School Spider aims to be as light touch as possible and only take data from the school that is absolutely necessary to perform the tasks we need.

All data is processed and stored within the EU and where possible stored in UK data centres.

Statement of assurance

School Spider will ensure that:

1. We will put in place measures to protect customer information from a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
2. We will meet our regulatory and legislative requirements.
3. We will produce, maintain and test Business continuity plans.
4. We will provide information security training to all our staff
5. We will report and investigate information incidents (whether actual or suspected), in line with our Incident reporting procedure.
6. We will monitor compliance with our Information Security Policy.

IRIS ensures that all employees comply with corporate standards and procedures. These include incident handling, information backup, system access, virus controls, passwords-authentication, communication and encryption. These policies are communicated to all employees via the company compliance portal and intranet.

School Spider Organisational Security

School Spider adheres to all GDPR regulations and has a Cyber Essentials Certification for IT setup and use. School Spider holds PCI DSS V 4.0 Compliance.

School Spider is part of the IRIS Software Group.

Organisational security at IRIS Group level

Data protection and information security at IRIS Software Group is controlled by the *IRIS Privacy, Security and Compliance Steering Group*. This group meets at least quarterly and includes:

- Members of the Executive Committee
- The Chief information Officer (CIO)
- IRIS Group IT Director
- IRIS Group Data Protection Officer
- IRIS Group Compliance Manager
- Other key security leads within the company

The Privacy, Security and Compliance Steering Group approves IRIS Group level policies relating to information security and data protection, which IRIS products must comply with. There are three Group policies and a detailed Information Security Management System (ISMS). The three Group level policies are:

- IRIS Group Data Protection Policy – this sets out the roles and responsibilities for data protection compliance within the IRIS Group. It also sets out the requirement for risk assessment and data protection assessment for all projects and proposals that will change or impact on the handling or use of personal data.

- Information Security and Acceptable Use Policy Summary – this sets out the basic information security and acceptable use standards that all staff within the IRIS Group are required to adhere to.

- IRIS Personal data incident reporting and investigation procedure – this indicates the reporting and investigation procedure for all security incidents that become known or are reported to anyone within the IRIS Software Group.

The above policies are communicated to all staff and relevant external staff within the IRIS Group at least annually, using a dedicated training and policy management platform. Managers responsible for delivering IRIS products and services are required to ensure local arrangements are in place to comply with those policies and to evidence this.

- IRIS ISMS – This is the default security system for IRIS Software Group. All IRIS products must meet or be working towards meeting the standards of the IRIS ISMS except for those which already have their own certification under ISO27001 or any other standard relating to information security and data protection.

Organisational security for School Spider by Iris

At School Spider the product manager is the single point of contact for routine security and data protection enquiries. They work with the managers involved in delivering School Spider to ensure School Spider complies with the IRIS Group policies and ISMS or any other information security standard – as well as any other regulatory requirements relevant to the service.

For School Spider, the team with responsibility for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

- School Spider Product Director – Alex Ellis
- School Spider Development Manager – Stephen Slack
- School Spider Support Services – Tracey O'Brien

The School Spider team keep your data secure by ensuring that appropriate measures are implemented to protect your data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to your data while being stored, transmitted or otherwise processed by or on behalf of School Spider.

Measures are "appropriate" if they have been identified through risk assessment.

The School Spider team will ensure adequate records are created and maintained to support compliance verification and inspections and incident response (subject to any limitations set out in our Terms and Conditions).

The IRIS Group Data Protection officer is responsible for providing advice and guidance to the School Spider team and for monitoring our compliance on all security policies and related issues. The IRIS Group Data Protection Officer is also the designated contact for the Information Commissioner's Office.

Group Operations are responsible for the operation and integrity of School Spider's IT systems and for keeping systems reasonably up to date.

School Spider's Development systems are managed by a 3rd party hosting provider. School Spider is hosted on dedicated hardware in EU data centres.

Asset register: Dev Ops Directorrecords and maintains a register of all assets, relevant to School Spider (including acquired software licences) in a fixed assets system.

Client defined classifications: Client information and materials processed, stored or transmitted by School Spider shall be handled strictly in line with the customer's prior advised classification policies and standards, subject only to legal compliance

School Spider human resource security

School Spider staff will have access to your school's data.

Prior to employment

- Staff and contractors are subject to background checks and verifiable references to ensure suitability for any given job role.

- All staff are required to accept our Group Data Protection Policy, Incident Reporting Procedure and Information Security & Acceptable Use Policy.

During employment

- All staff are required to complete mandatory training regularly (at least once every 12 months) regarding data security, 3rd party access, phishing and social engineering attacks. Corporate policies and training are delivered using a system called KnowBe4 and completion is expected within 14 days of the material being made available. Adherence to this policy is monitored and controlled in employee 1:1's and performance reviews.
- All staff are required to follow the internal Incident Management process should a data breach occur, with full investigation and follow up carried out by an internal Incident Management team:
- All of our employees have completed training around data protection and how to identify a data breach along with the responsibility to report any breach to our data protection officer.
- If the data breach involves any schools data, we will inform the signatory (or suitably senior official at the school) of the data breach within 8 hours.
- If the breach is reportable under GDPR, it will be reported by our data protection officer (via our data protection management tool) to the ICO within 72 hours.

Termination and change of employment

- Upon instruction from HR of a person leaving School Spider by Iris, that person's access to confidential areas shall be restricted immediately, culminating in:

    - full removal of access to any part of the corporate network prior to departure,
    - all corporate assets in that person's possession having been returned and or been collected by the relevant Department manager or the Information asset Owner as appropriate.
    - In the event of a person transferring from one department to another within IRIS Software Group that person's access will be varied accordingly.

School Spider Access Control

School Spider Access Control is managed within the product for user roles. When a new customer is onboarded they nominate at least one user to be the privileged/admin user who can then assign these privileges to other users.

Authentication is managed using username and password, with multi factor authentication enabled for all staff user.

For the avoidance of doubt, School Spider by Iris warrants to Clients that it will not seek to circumvent, compromise or change the Client's security controls, and School Spider by Iris will not change the Client's software configurations (without proper authorisation); and no 'back door' password or other method of remote access into School Spider by Iris's software shall exist.

Encryption (cryptology)

All data is encrypted in transit using 256 bit SSL encryption. Data backups are encrypted at rest.

School Spider physical and environmental security

School Spider physical servers are hosted in UK Rackspace data centres and restricted by biometric authentication and 24x7x365 surveillance.

Firewalls, intrusion detection tools, access logs and user logging are all in place to maintain the highest possible level of security.

Media handling

Management of removable media – We do not use removable media at School Spider

Disposal of media – All media on a staff machine is deleted after the need for it has passed, this will be automatically deleted from the trash can when it is emptied.

Operations security

All data is backed up nightly, and regular tests are undertaken to ensure that service can be restored from backups as part of the hosting providers Disaster Recovery process.

Change Management processes are in place to review and approve any changes made to products, environment and infrastructure.

Capacity is monitored automatically and any notable changes highlighted and reviewed. Development is carried out on separate environments, for engineers, testing and then being deployed to production environments.

School Spider uses tools to detect malicious software and all connections to machines containing PII are only authorised from the corporate VPN. This VPN requires an email, password and MFA to access.

Firewalls and firewall rules are in place and access is logged and actively monitored.

System administrator and system operator activities are logged, and the logs protected and regularly reviewed.

PEN testing is carried out at least annually, and automated software is in place to detect vulnerabilities in both our software and third party dependencies.

Communications security

All School Spider data servers are located behind a VPN, firewall and access control. Users are limited to read-only access where possible. Where higher access levels are required this is granted at the lowest possible level and for a limited time.

School Spider has a policy in place for the acceptable use of email, instant messaging and other electronic communications. No PII is permitted to be shared via email and can only be shared using our customer case management platform.

System acquisition, development and maintenance

All new information systems, features and suppliers go through a thorough review process. This includes, but is not limited to:

- System architects

- Security specialists

- Engineers

- Product Managers and Owners

- Support, on-boarding and professional services teams

Security in development and support processes

Security is foremost in all phases of software development and documented in a secure development policy. Solution designs are reviewed by Architects and security specialists and automatic code and vulnerability scanning is in place.

All system changes are controlled by the use of formal change control procedures, meeting weekly to review and discuss planned changes. Where changes are needed urgently a shorter, more succinct process is in place and procedures are in place to review where a high occurrence of urgent changes are requested for a particular product.

Application systems are automatically tested after changes to the operating system.

Once changes are released both automated and manual testing is completed to validate the change being made and to ensure that other negative changes have not been introduced.

Test data

School Spider uses test data which is generated randomly and is not associated with any customer or data subject. Where staff need to use real contact information for testing access to this is limited and regularly reviewed.

Processing locations and international data transfers

On occasion, IRIS may use engineers and third parties located in India for production environment support, deployment activities, access management and security & vulnerability management. In all these instances, information is held on secured network drives held in the UK and only accessible by those authorised to process it. All relevant security requirements have been addressed and further information is available on request. A full risk assessment is carried out annually to ensure that client data is always protected.

Supplementary measures for personal data processed in India

IRIS and its engineers in India adhere to the standards of ISO 27001 and uses privileged access management controls to audit activity of engineers. VPNs and Bastions are used where appropriate and all communications are over encrypted channels. IRIS has an international data transfer agreement in place with all sub-processors used that are based in India. This requires them to comply with IRIS data protection and security policies and standards, particularly in relation to handling requests from official sources.

Supplier relationships

Information security in supplier relationships

All suppliers are reviewed regularly to ensure that access is still required

Supplier service delivery management

Monitoring and review of supplier services – IRIS works closely with suppliers to ensure service delivery and continued quality.

Managing changes to supplier services – IRIS has management procedures for authorising and implementing changes to supplier services including whether information security policies, procedures and controls are managed in accordance with its classification.

Summary of sub-processors

Postmark (email sending)

Text Anywhere (SMS provider)

Gainsight (in-product help and analytics)

Clover (payment processing)

Cybage

Digital Ocean (Software hosting)

Google (Push notification sending & translations)

Information security incident management

Management of information security incidents and improvements

All staff are required to follow the internal Incident Management process should a data breach occur, with full investigation and follow up carried out by an internal Incident Management team:

- All of our employees have completed training around data protection and how to identify a data breach along with the responsibility to report any breach to our data protection officer.
- If the data breach involves any schools data, we will inform the signatory (or suitably senior official at the school) of the data breach within 8 hours.
- If the breach is reportable under GDPR, it will be reported by our data protection officer (via our data protection management tool) to the ICO within 72 hours.

All staff are required to follow the IRIS Group Incident Reporting Procedure to report security incidents to their department lead as quickly as possible and to raise a major incident via Teams, email or phone to the central Incident Management Team.

Information security problems and issues are reviewed regularly in team meetings and a join decision made on whether to classify them as information security incidents that need to be reported through the corporate procedure.

Reports of breaches or suspected breaches are raised to our support team, usergroup or by email and these are prioritised and investigated immediately. Investigation can be carried out by support sessions, reviews of user and access logs and data comparison. If a breach is found to have taken place the documented incident process is followed and assistance requested from the Data Protection Office.

All critical incidents have a root cause analysis completed once the incident is closed and mitigating or supporting work identified and monitored by the Incident Management Team.

Business continuity – Information security aspects

Information security continuity

All data is backed up 4 hourly, and regular tests are undertaken to ensure that service can be restored from backups as part of the hosting providers Disaster Recovery process.

Disaster recovery, business continuity and data integrity processes are in place and reviewed regularly and monitored by DevOps, architects and security personnel.

Redundancies

Availability of information processing facilities – redundancy is built in to the School Spider infrastructure, with load-balancing, backup of both data and hardware and primary and secondary sites in place to ensure that failover could be achieved should a problem occur.

Compliance

Compliance with legal and contractual requirements

Identification of legislation and contractual requirements applicable to School Spider – IRIS is committed to providing high-quality, secure and compliant products. We comply to all relevant legislative and contractual requirements including GDPR and industry certifications such as Cyber Essentials and ISO certification. IRIS uses relevant software to help us maintain records related to this and to ensure that reviews are conducted regularly and by the relevant staff levels.

Important records of the organisation are protected from loss, destruction, falsification unauthorised access and unauthorised release.

Privacy and protection of personally identifiable information – IRIS' Privacy Policy is documented and published on our website here: https://www.iris.co.uk/privacy-policy/

Information security reviews

Independent review of information security – IRIS Privacy and Data Protection policies, processes, procedures, controls and control objectives are subject to regular independent reviews at planned intervals or when significant changes occur.

Technical security reviews are carried out using manual and automated tools to confirm information security objectives are achieved – this is achieved by regular PEN testing, vulnerability scanning, pipeline scanning and manual reviews of solution design and code.

Data Protection – quick reference

IRIS Group Data Protection Officer - Vincenzo Ardilio - dataprotection@iris.co.uk

Data protection owner for School Spider – Alex Ellis – alex.ellis@iris.co.uk

We will make your personal information available within the IRIS Software Group on a need-to know basis in order to achieve our legitimate business objectives. If we have sub-contracted any aspect of the product or services you are using, we may need to share your details with the relevant supplier, also on a need to know basis.

Location of personal data processing, hosting and access by IRIS agents

On occasion, IRIS may use engineers and third parties located in India for production environment support, deployment activities, access management and security & vulnerability management. In all these instances, information is held on secured network drives held in the UK and only accessible by those authorised to process it.

Retention of data

School Spider is committed to the protection of data held whilst customers are accessing the system.

- If a customer cancels their agreement, their school setup is deleted from the IRIS School Spider system, meaning that all personal pupil and staff data is removed. The school is asked to remove all related software from their school systems.
- The Company will retain history for a 60 day period before it is destroyed, in case of a later need on the school's part to access this information. During this period, all this data will be retained on secure back-up systems.

- No paper copies of pupil or staff data are held at any time by School Spider. Access is solely via our secure systems for the purposes of guaranteeing Project Partners' full and comprehensive use of the system and to realise our aim of effective, first class customer service.

Data subject rights

We are fully committed to support schools with any rights of access requests they have. This may come from a parent, student or member of staff at the school. We will respond to requests without undue delay and within one month of receipt.

There are specific audit trails in the system to allows the user to export historical contact data from the system.

We can export and share data, with written consent, in common formats like Excel and Word.