IRIS BioStore -Portal Cashless

Information Security Assurance Statement [data processors]

Document control	
Version number: 1.0	
Owner:	Beverley Thompson & Allana Jones
Date of last update:	12/03/2025
Document type:	
Replaces:	
Approved by:	
Approval date:	
Data protection impact screening:	
Date of next formal review:	

Contents

[Product/service name] information security statement

Information security assurance statement

Objective of this document

The purpose of this information security assurance statement is to provide customers of IRIS BioStore Portal Cashless Catering, 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 IRIS BioStore Portal Cashless Catering as a thoroughly secure software and service provider.

Description of the data processing carried out by IRIS BioStore Portal Cashless Catering

IRIS BioStore Portal is a native cloud-based cashless catering solution designed for educational institutions, specifically schools and universities. It facilitates a cashless system for students to pre-order, pay for, and collect their meals during lunchtime.

- **The nature of any processing of personal data.**
  IRIS BioStore Portal is hosted by IRIS using RACKSPACE Cloud, a cloud-based secure storage facility. IRIS BioStore Portal provides establishments/organisations the ability to enrol students and staff in a central database to allow use of the Portal cashless catering solution. Using QR cades and pin as authentication methods. IRIS BioStore integrates with third-party payment providers to enable students to pay for lunches linked to our cashless solution.
- **The purpose of the processing.**
  IRIS BioStore Portal processes reports concerning School Meals (FSM) uptake, reconciliation, top sellers, staff meal uptake for the data controller. The historical data is securely archived and maintained on the cloud-based server hosted by IRIS through RACKSPACE Cloud for BioStore Portal Cloud solution. Access to the data is restricted to the IRIS BioStore support team and engineers, who all undergo Disclosure and Barring Service (DBS) checks as IRIS employees. The

establishment or organisation retains ownership of the data, and IRIS BioStore strictly guarantees that data sharing never occurs without explicit consent.

- **The type(s) of personal data that being processed.**
BioStore Links with IRIS Sync and is used to export data from the organisation's Management Information System (MIS). How IRIS Sync is set up depends on the MIS used by the organisation. The data controller (organisation) needs to set the permissions required for IRIS BioStore Portal to extract the data.

Where IRIS BioStore Portal does not have direct integration, we use Wonde, a third-party data supplier. We are an accredited technical partner of Capita SIMS and have similar arrangements with other providers. Organisations have complete control and can terminate the automatic data sharing at any time.

IRIS Sync software requires minimal IT administration but if help is required, a dedicated team of support staff are available to assist.

Security
IRIS School Data Extractor is end-to-end encrypted.

School Management Information System (MIS) store the following information that IRIS BioStore Portal process: -

- Personal Information of students' details stored within the Management Information System**:**
  - Name
  - Address
  - Home telephone /mobile numbers
  - Date of Birth
  - Gender
  - Class, Year group, Registration group, School House group
  - School photograph records
  - E-mail addresses
  - Attendance records
  - Free school meal allowance

- Personal Information about establishment/organisation employees:
  - Internal Management Information System (MIS) record ID
  - Name and Title
  - Gender
  - Date of Birth
  - Salutation
  - Association with class, lesson, year, registration, or house groups
  - Mobile, home and work phone numbers
  - E-mail addresses
  - photograph records
  -
- **The type(s) of people that are the subjects of the information being processed.**
  - Employees, students and Parents who have opted into the establishment/organisation Management Information System (MIS).

Statement of assurance

IRIS BioStore 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.

IRIS BioStore Portal Organisational Security

The management arrangements in place to ensure that our BioStore Portal product is managed securely and compliantly are comprehensive and prioritise safeguarding data integrity.
Establishments/organisations are guided on how to request access to their data through email, subject data access, or via the IRIS BioStore helpdesk. They have the capability to rectify data discrepancies using their Management Information System (MIS) and hold the authority to erase or request data erasure from IRIS BioStore.
As data controllers, they can opt to restrict processing to specific functions and are required to provide consent for certain data sets and processes. IRIS BioStore adheres to processing legitimacy and contractual agreements, collecting only necessary data for system usage and report processing.
Data is encrypted at all stages - storage, usage, and transfer- with restricted access limited to essential IRIS BioStore personnel.
Strong password protocols are enforced, and security measures are in place to protect sensitive data.
Data processing and access are primarily handled by UK-based IRIS employees, with minimal access granted to the Knowledge Process Outsource Team (KPO) in India.
Customers utilising the cloud-hosted Cashless solution can seek data management support via the Service Cloud support tool. Additionally, customers are empowered to manage requests from parents/carers regarding personal data within the IRIS BioStore product or through the support ticket system.

IRIS BioStore Portal 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 IRIS BioStore Portal

At IRIS BioStore Portal, the Product Manager is the single point of contact for routine security and data protection enquiries. They work with the managers involved in delivering IRIS BioStore Portal to ensure IRIS BioStore Portal 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 IRIS BioStore Portal, the team responsible for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

- Mand Becket - Product Management Manager

- Bev Thompson - Product Manager
- Allana Jones - Product Owner
- Stephen Slack - Senior Manager, Engineering
- Jonathan Blake – Software Engineer Team Lead
- Tracey O'Brien- IRIS BioStore Support Services

The IRIS BioStore Portal 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 IRIS BioStore Portal.

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

Date of last IRIS BioStore Portal risk assessment review: 20-05-2024

The IRIS BioStore Portal 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 IRIS BioStore Portal 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.

Development Operations and the IRIS BioStore Product Owner are responsible for the operation and integrity the IRIS BioStore cloud-hosted solution for Cashless and for keeping systems reasonably up to date.

Cloud hosted IRIS BioStore Portal, Development systems are managed by an Internal Development Operations team and the IRIS BioStore Product Owner.

Asset register: Dev Ops records and maintains a register of all assets, relevant to IRIS BioStore Portal (including acquired software licences) in a fixed assets system.

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

IRIS BioStore Portal human resource security

IRIS BioStore Portal staff will have access to your [customer'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:
  o 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.
  o 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.
  o 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 IRIS, that person's access to confidential areas shall be restricted immediately, culminating in:

  o full removal of access to any part of the corporate network prior to departure,
  o 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.
  o Immediate removal of access to Office applications, including email, Teams and OneDrive
  o In the event of a person transferring from one department to another within IRIS Software Group that person's access will be varied accordingly.

IRIS BioStore Portal Access Control

IRIS BioStore Portal is able to set permissions to restrict access to all areas of the data, so only staff of the organisation with legitimate cause can access data. We recommend to our customers a password consisting of a minimum of 1O characters and must not be the same as the previous 4 passwords.

IRIS BioStore Portal can allow users to be assigned to an administrator role within the system, this user can access all areas and features with no limitation. The details of who is assigned to the Administrator Role can be viewed and managed within Portal.

Authentication is managed using a leading authentication platform, Okta, which has rules and controls set for minimum password strength, management and suspicious activity. New users are sent an email which requires them to set their password before being able to access the product.

IRIS BioStore Portal Staff Access Control

The IRIS BioStore team use Service Cloud, a support ticketing system, SalesForce, our Customer Relationship Management System, and Office 365. All systems require password authentication for access. Access is only granted to employees of IRIS BioStore with legitimate need.

If an employee leaves, their access to the systems is revoked by central IT.

All IRIS BioStore source code is restricted using source control, which provides a full audit trail of changes.

For the avoidance of doubt, IRIS BioStore ensures to customers that it will not seek to circumvent, compromise or change the customer's security controls, and IRIS BioStore will not change the customer's software configurations (without proper authorisation), and no 'primary' password or other method of remote access into Iris BioStore Portal's software shall exist. Multi-factor authentication is required for those with administration privileges within the Okta platform.

Encryption (cryptology)

All data is currently 256bit Advanced Encryption Standard (AES) encrypted.

IRIS BioStore Portal physical and environmental security

IRIS BioStore Portal Cashless Catering solution, which is hosted by IRIS using RACKSPACE Cloud, a cloud-based secure storage facility which is restricted by biometric authentication and 24x7x365 surveillance.

IRIS SYNC stores data securely within Amazon Web Services (AWS).

All IRIS BioStore employees work from home. IRIS BioStore has stringent policies and procedures in place for home working as set out in the Group IT Working from Home Manual, all employees working from home follow the IRIS Permanent Remote Working Policy.

All employees are required to accept our:
- Group Data Protection Policy
- Incident Reporting Procedure
- Information Security and Acceptable Use Policy
- IRIS Confidentiality Policy

Equipment

IRIS BioStore staff adheres to the IRIS company Computer Systems and Equipment Use Policy

Laptops, tablets, and other devices are provided to IRIS BioStore employees who require mobile computing or remote work capabilities, adhering to relevant IRIS Policies. These policies encompass various aspects such as physical security protection, communication capabilities, preference for a virtual desktop environment, information security with encryption, measures to prevent unauthorised access by friends and family, maintenance support and updates, anti-virus and firewall requirements, insurance prerequisites, backup procedures, and business continuity processes. Additionally, the policies outline protocols for the return of equipment when requested, ensuring the secure and efficient use of technology resources by IRIS BioStore staff.

Media handling

IRIS BioStore adheres to the IRIS company Computer Systems and Equipment Use Policy

Operations security

We recommend to our customers a password consisting of a minimum of 10 Characters and must not be the same as the previous 4 passwords.

Within the solution IRIS BioStore can allow privileged users by updating the permissions set within the application software. The details of who and what data can be accessed by a privileged user is accessible to the customer within the help files stored in the application software. For cloud hosted IRIS BioStore Portal, the customer can request from the IRIS BioStore support, credentials to allow them to amend access themselves. An audit trail is kept in the support ticketing system in Service Cloud.

The IRIS BioStore team use Service Cloud, a support ticketing system, SalesForce, our Customer Relationship Management System, and Office 365.All systems require password authentication for access. Access is only granted to employees of IRIS BioStore with legitimate need.

If an employee leaves, their access to the systems is revoked by central IT.

All IRIS BioStore source code is restricted using source control, which provides a full audit trail of changes.

For the avoidance of doubt, IRIS BioStore ensures to customers that it will not seek to circumvent, compromise or change the customer's security controls, and IRIS BioStore will not change the customer's software configurations (without proper authorisation), and no 'primary' password or other method of remote access into IRIS BioStore Portal's software shall exist.

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.

IRIS BioStore 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.

Communications security

All IRIS BioStore 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 table-by-table. Each customer has its own unique identifier and has its own set of tables based on that identifier. The system is designed to only allow users from that customer's organisation access to their own tables, hence only their own data.

IRIS BioStore 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.
All 3rd party suppliers, vendors and contractors have confidentiality or non-disclosure agreements in place which are reviewed, documented and reflect the product/service's needs for the protection of information.

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:

- o System architects
- o Security specialists
- o Engineers
- o Product Managers and Owners
- o 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

IRIS BioStore 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

All new suppliers and contractors complete an in-depth new supplier security Due Diligence document, which is reviewed by the IRIS IT Security Team to ensure our strict compliance procedures are met. The Due Diligence document covers the following:

- o Information Security Policy
- o Integration with IRIS BioStore software
- o Access Controls
- o Training
- o Education and Training
- o Asset and Inventory Management
- o Environment and Network
- o Data Information and Security

Supplier Service Delivery Management

Monitoring and review of supplier services.

Quarterly meetings are held with all suppliers where the agenda is:

- o Current Service Levels
- o New ideas for Product
- o Current functionality of product

All new product requests and services have a process to be signed off by the IRIS BioStore Chief Financial Officer and Senior Product Director.

List of third parties and sub-processors involved in IRIS BioStore processing of customer data [correct as at 10/03/2025]

Summary of sub-processors

Universal Smart Card	Card printing services	Product
Osborne Technologies Ltd	Visitor System	Product
GroupCall	Data extraction for use with partners where full integration is not in place	Product
Payment Sense	Card Payments - for use alongside Cashless	Product
Wonde	Data extraction for use with partners where full integration is not in place	Product
IRIS Sync	Data extractor	Product
ISAMS	Management Information System (MIS)	Product
Digital ID	Card Printing	Product
RACKSPACE	Cloud Storage	Product
Amazon Web Services (AWS)	Management of Websites and Apps	Product
OKTA	Secure Identity Management	Product

Service Cloud	Support Ticketing system	Product
SalesForce	Customer Record Management System (CRM)	Product
Product IRIS ParentMail	On-line payments	Product
Gainsight	Analytics	Product
ParentPay	Payment provider	Product
Apple	App hosting (Tills/Bookings)	Product
Android	App hosting (Tills/Bookings)	Product
Cybage	External Development Team	Product

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:

- o 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.
- o 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.
- o 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 joint 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, user group 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 is identified and monitored by the Incident Management Team.

Business continuity – Information security aspects

IRIS BioStore Portal Follows the IRIS Business Continuity Policy

This policy document defines a broad framework for the implementation of IRIS Group's BCMS to minimise the impact of business disruption. Full compliance with this policy will ensure procedures exist for recording, assessing and managing business continuity risk; identifying and prioritising essential activities; responding to business disruptions or incidents, regardless of cause; and maintaining essential services (or restoring services to a minimum acceptable level). This policy is built on current good practice and is intended to:

- o Improve Business Continuity Management (BCM) resilience within IRIS.
- o Ensure through the adoption of resilience principles, the continuous operational delivery of critical services when faced with a range of disruptive challenges such as staff shortages, denial of access and failures in key suppliers.
- o Help drive a unified and cohesive approach to BCM which parallels with ISO22301 and develop resilience within IRIS.

Information security continuity

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.

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 into the IRIS Sync 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 IRIS BioStore Portal– 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.

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 IRIS BioStore - Allana Jones- Allana.jones@IRIS.co.uk,

Bev Thompson- Beverley.thompson@IRIS.co.uk

Jon.blake – jon.blake@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

Customer personal data will be processed or stored in the EU.

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

IRIS BioStore 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 BioStore Portal system, meaning that all personal pupil and staff data is removed.

No paper copies of pupil or staff data are held at any time by IRIS BioStore. 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.
- We can export and share data, with written consent, in common formats like Excel and Word.