Staffology HR

Information Security Assurance Statement Staffology HR

Document control
Version number: **1.0**
Owner: **Jonathan Low – Product Manager**
Date of last update: **27/12/2023**
Document type: **Assurance Statement**
Replaces: **N/A**
Approved by: **Julian Musson – Senior Product Manager**
Approval date: **TBA**
Data protection impact screening: **N/A**
Date of next formal review: **27/12/2024**

Information security assurance statement

Objective of this document

The purpose of this information security assurance statement is to provide customers of Staffology HR and IRIS HR Professional (to be known from now on as Staffology HR) 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 Staffology HR as a thoroughly secure software and service provider.

Description of the data processing carried out by Staffology HR

Staffology HR is a comprehensive cloud-based HR and payroll software solution that helps businesses of all sizes manage their employee information, payroll, and HR tasks efficiently. It provides a single platform for managing all aspects of employee lifecycle, from recruitment and onboarding to performance management and exit processes.

Statement of assurance

Staffology HR 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.

Staffology HR Organisational Security

Staffology HR 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 Staffology HR

At Staffology HR, the product manager is the single point of contact for routine security and data protection enquiries. They work with the managers involved in delivering Staffology HR to ensure Staffology HR 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 Staffology HR, the team with responsibility for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

Name	Department	Role
Julian Musson	Product	Senior Director Product Manger
Jonathan Low	Product	Product Manager
Mohammad Othman	HCM Engineering	Engineering Director, Staffology
John Cooper	HCM Engineering	Engineering Manager, Staffology
Thomas Derbyshire	Customer Service/Support	Senior Manager, Customer Services
Paul Shorrock	Professional Services	Implementation Manager
Tarka Duhalde	Finance and Accounts	VP, Financial Controller
Rob Brough	Sales Order Processing	Director, Revenue Operations
Vincenzo Ardilio	Central Compliance	Data Protection Officer – Group

The Staffology HR 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 Staffology HR.

Measures are "appropriate" if they have been identified through risk assessment.
Date of last Staffology HR risk assessment review: **October 2023**

The Staffology HR 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 Staffology HR 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 IT are responsible for the operation and integrity of Staffology HR's IT systems and for keeping systems reasonably up to date.

Staffology HR's Development systems are managed by a local internal development team.

Asset register: Group IT records and maintains a register of all assets, relevant to Staffology HR (including acquired software licences) in a fixed assets system.

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

Staffology HR human resource security

Staffology HR 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

The responsibility for ensuring that processes and procedures are both established and maintained are held with Staffology HR Managers. Employees, third parties and contractors are mandated to read, and sign a document to confirm understanding of their responsibilities. In the event of the use of an external party, controls are put in place to restrict the level of data they have access to in line with group policy and this activity is supervised and relevant risk assessments have taken place.

In addition to local procedure, IRIS Group also require the completion of corporate policy training and the subsequent testing of this knowledge through the KnowBe4 portal. This testing is repeated as frequently as is reasonable for all employees, third parties and contractors.

In the unlikely event of a security breach, the governing policy or procedure would be rereviewed and amended to ensure stricter compliance moving forwards. Staffology HR places the onus on the employee for their adherence to security protocols and a disciplinary procedure is enforced for non-compliance. If no improvement is found to employee performance under the afore mentioned disciplinary, employment is terminated as set out in the terms of the procedure.

Staffology HRTermination and change of employment

In the event of an employee terminating their employment contract with IRIS, the following departments are notified and the following actions take place:

Department	Action
Staffology HR Management	To notify Group HR and Group IT, revoke log in credentials from internal systems required for role.
Group HR	To restrict access to internal systems, HR portal and notify Payroll.
Group IT	To close off network access, organise recovery of assets, revoke other access (Office 365 account, Cloud accounts, VPN access).

Upon instruction from HR of a person leaving Staffology HR, 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.

All employees have been contracted to a non-disclosure clause in their contracts that still remains applicable after termination.

Staffology HR Access Control

The purpose of the Access Control Policy is to ensure that information systems resources and electronic information assets owned or managed by IRIS are available to all authorised personnel. The Policy also deals with the prevention of unauthorised access through managed controls to create a secure computing environment.

Access controls to network, operating system and applications shall be set at an appropriate level on need to use basis, which minimizes information security risks yet allows the business activities to be carried without undue hindrance. This is managed as per the Organisational Security section in conjunction with the IT Manager and Information Asset Owner and in accordance with the IRIS Group Access Control Policy.

Access is granted on the least privileged rule basis consistent with an individual's job/role responsibilities. For Staffology HR user login, system enforced password complexity rules ensure that strong passwords are used and Users are responsible for keeping them confidential. Systems and information should be secured whenever left unattended.

In addition we also offer Single Sign On (SSO) with Staffology HR for both internal and external users.

All static user equipment must be kept in good order and used responsibly; all laptops shall be subject to the IRIS Group's Acceptable usage policy. Passwords must not be disclosed to colleagues or any third parties. As set out in IRIS Group's standard HR Policies all personnel must maintain full conformance with company undertakings in respect of confidentiality.

Access to cloud-based administration consoles for privileged IRIS' IT Department and IRIS users is mandated with password authentication.

Server Operating System Access Control along with change and patch management shall at all times adhere to Microsoft's best practice and shall be administered by the IRIS IT team in conjunction with the Infrastructure Managers in respect of their individual department's development and support environments.

All administration systems are monitored, and audit trails produced together with email notification to the System Manager of any unauthorised attempts to access the corporate network.

Remote access to a client's network shall always be subject to client's prior written (or otherwise validated) consent or request and must be controlled either by using clients provided VPN and or remote assistance software which utilises SSL and provides a full audit trail.

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

For additional information regarding Access Control please visit our help centre's security section

Encryption (cryptology)

Personal data is stored in a combination of Azure Storage and Azure SQL with data encrypted at rest using 256-bit AES encryption using dedicated service-managed keys.

Refer to Azure Storage encryption for data at rest and Transparent data encryption for SQL Database, SQL Managed Instance, and Azure Synapse Analytics for more information.

All communication between client browsers and Staffology HR is protected by TLS 1.2 encryption

For additional information regarding Processing Data please visit our help centre's security section
For additional information regarding Encryption please visit our help centre's security section

Staffology HR physical and environmental security

Staffology HR follows guidance set out in our group Physical Access policy.

- Physical entry controls - Entry to the site is restricted to key fob or key pad entry. Only IRIS employees have access to the area payroll is completed in.
- Securing offices, rooms and facilities – Physical security is employed at greater levels where higher risk or classification of a more sensitive nature of data is identified.
- Protecting against external and environmental threats - Staffology HR has a robust business continuity plan, however we also place a great importance on our first defence. We are protected by a failover line in the event we lose connectivity due to environmental damage, we also have the ability to move the entire site remote or transfer ownership to a satellite office at a moment's notice.

IRIS Group have invested heavily into our cyber defences, these are controlled by IRIS Group IT. We have also moved customer data into an ISO-secure cloud-based environment which adds additional layers of security to your information.

IRIS became a paperless office in January 2020.

- Working in Secure Areas – In the event a third party needs access to a secure area within the physical site, they are escorted at all times by facilities. Additional measures are covered under the topic "Human Resources Security".
- Delivery and loading areas – Deliveries are taken at reception with no access granted to unauthorised people.

IRIS does not maintain physical servers or other infrastructure for Staffology HR. All infrastructure is hosted by Microsoft Azure, and as such, Staffology HR inherits the physical and environmental controls implemented by Microsoft. Details may be found on the Microsoft website.

Access to IRIS resources and equipment is subject to Group IT Policies.

For additional information regarding Business Continuity please visit our help centre's security section

Equipment

Equipment	Description
Equipment siting and protection	Access to critical computing resources or infrastructure is physically restricted to authorised personnel with access controlled by keys, swipe cards or a key pad lock.
Protection against power failures and disruptions	The physical site has taken adequate measures to prevent disruption. Installation of a failover line in the event of loss of connectivity.
Equipment maintenance	Regular maintenance is carried out on equipment as per the recommendations of the manufacturer. A maintenance log is held on site and maintained by designated Facilities personnel.
Removal of assets	Any physical assets to be moved from one place to another place within the office and outside the office must require prior approval from Senior Management. A register of all assets taken off site is kept and maintained by the Site Leader and shared with Group IT.
Security of equipment and assets off-premises	assets off-premises Guidance is outlined in mandatory policy document.
Group IT: Working from home manual	With considerations on Information Security, use of the Group's VPN. Two Factor Authentication is implemented for access to all secure areas of the network.
Unattended user-equipment	Staffology HR enforces a clear desk policy. Staff laptops & IT assets are sited in a secure office area, information displayed on screen may be confidential. All computers revert to screen saver mode at timely intervals and staff are mandated to logoff from sessions and ensure any paper is securely disposed of
Clear desk and screen policy	Staffology HRSince going paperless in January 2020, in line with our Clear Desk Policy, employees and contractors are made aware of their responsibilities to ensure that data is protected at all times, we also have locked shredding cabinets for the secure disposal of notepads and post-it notes, if required. All employees and contractors are expected to lock their computer screens, as a redundancy procedure, IRIS Group IT set screens to auto lock after 5 minutes and will require a password from the user to unlock.

Media handling

Media Handling	Description
Management of removable media	Staffology HR sets out the acceptable usage of removable media in Information security and acceptable use summary Policy. It is not permitted to create a copy of protected data on unauthorised devices
Disposal of media	Staffology HR sets out responsible use of data in our IRIS Data Protection Policy, including secure disposal and audit of media

Operations security

Operations Security	Description
Documented operating procedures	Backups, transmission of information between environments and equipment maintenance are all fully managed services by suppliers listed in this document. All suppliers are independently audited against ISO 27001 standards.
Change management	Change management controls have been implemented to ensure satisfactory control of all changes. Major architectural changes are reviewed by an architecture review board (ARB) to discuss security, service level and complexity issues.
Capacity management	Resources are monitored, tuned and protections made of future capacity requirements to ensure systems continue to perform at optimum levels.
Separation of development, testing and operational environments	Development and production environments are separated and managed through documented and automated deployment pipelines. Access to infrastructure is restricted through IP restriction lists. Desktop payroll developers do not have access to production environments, unless authorised for a specific purpose i.e. Product Support
Protection from malware	Staffology HR utilises Kaspersky, to protect against malicious software and this is centrally monitored. All client machines are auto updated on connection to the network or via internet. Firewalls are in place. Mimecast is used to provide comprehensive email filtering (not only to preclude spam but also to scan attachments more effectively to counteract viruses and other malware).
Back-ups	Both environment and software products have independent audit logs of activities carried out within each. Environment audit is maintained and monitored at Group IT and Infrastructure level and Product is reviewed by Staffology HR Management.

Protection of log information	IRIS Group IT controls clock settings, ensuring that synchronisation is enabled to a real time clock set at local standard time
Control of operational software	Installation of software on desktop payroll production systems is managed through package managers to minimise the risk of corruption of operational systems
Management of technical vulnerabilities	Penetration testing for integrated web-applications is planned annually to be undertaken by a third party. Security is considered during backlog refinement and discussed as part of the overall product backlog and workload. Any changes which have security implicants are reviewed by the Architecture Review Board.
Restrictions on software installations	Group IT regularly review acceptable use and monitor or restrict installations that have not yet been deemed safe. Requests to install new software must be authorised by Group IT if not already placed on a safe list.

For additional information regarding Operations and Equipment please visit our help centre's security section

Communications security

Communications Security	Description
Network security	All integrated web-applications are maintained and tested to a high standard of security. The integrity of client data is ensured through a quality hosted environment that holds more than appropriate accreditation outlined within this document
Security of network services	We employ the use of Cloud-Based Technology that houses personal data in UK Data Centres hosted by Azure, that uses world class security protocols to ensure security compliance (accreditation details in 'Organisational Security' section).
Segregation of networks	The network client data and software used to process this data are held in separate networks to mitigate risk. These networks are independent of all other business IRIS transacts and controls are in place to ensure that only authorised persons have access to these drives.
Electronic messaging	IRIS employees are subject to audited training on appropriate use of electronic communication, particularly with sensitive and/or personal information. In cases where customer information needs to be shared for fault finding purposes (such as support / develop liaison), these are controlled through restricted access CRM systems requiring multi factor authentication.
Confidentiality or nondisclosure agreements	As required, Staffology HR uses NDAs and maintains signed agreements to protect

	confidentiality. The requirements for confidentiality or non-disclosure are identified, reviewed, documented regularly by IRIS and communicated through training plans.

For additional information regarding Communication please visit our help centre's security section

System acquisition, development and maintenance

Securing application services on public networks - Where possible, integrated web-applications enforce the use of TLS 1.2 as a communication protocol. Security is considered during Architecture Review Board (ARB) stage for major projects; all code changes are subject to automated analysis against the OWASP top 10 and SANS top 25 lists. In addition, the codebase is scanned at least once a week by an automated vulnerability scan tool. Any issues found during any of these stages are fixed straight away, before release. The SDLC emphasises shifting security testing left so that the master branch remains secure, stable and releasable

Security in development and support processes

Security in Development and Support Processes	Description
System change control procedures	Major system changes are reviewed by the Architectural Review Board (ARB) mentioned previously in this document.
Technical review of applications after operating platform changes	IRIS test all product updates against a range of supported environments and software. Regression testing is completed to review the overall product impact of any system changes
Restrictions on changes to software packages	Changes to software development inhouse is subject to change control procedures.
Secure system engineering principles	Principles for engineering secure systems have been established, documented and maintained by the IRIS architecture team and are used as part of an internal training plan for all developers (Architecture Corpus)
System testing	All system and application changes are subject to an appropriate combination of manual, automated and regression testing comprised of testing suites managed by the internal quality engineers on the payroll team. All features are tested before being accepted through a series of environments before they enter the production environment
Secure development environment	The organisation has appropriately assessed the risks associated with individual system development and integration efforts that cover the entire system development lifecycle. Development environments are assessed for suitability and security by the Architectural Review Board.

For additional information regarding System Acquisition, Development & Security please visit our help centre's security section

Test data

Protection of test data - Copies of production databases are not used, and live production data is not used for testing purposes. Development, QA and staging environments have a series of stock / dummy data and manually entered data of fictitious companies and employees for the use of testing

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

Supplier service delivery management	Description
Monitoring and review of supplier services	Suppliers are independently audited by third parties against ISO 27001/9001 standards. IRIS review these audits and SOC reports annually to assess if supplier relationships meet the standards for continuation.
Managing changes to supplier services	In addition to the assessment of supplier audits, if a new supplier needs to be selected for any reason, the IRIS internal compliance team are responsible for choosing an appropriate supplier based on ISO 27001 standards. After appropriate assessment, the Group Compliance Manager is responsible for such decisions.

Summary of sub-processors

External Data Processors	Data Location	Description
Microsoft Azure Hosting UK	UK	Staffology HR Software and client data is held in a Microsoft Azure hosted environment. All security protocols and accreditations are mentioned previously within this document.
Jira Atlassian	UK	Staffology HRs development lifecyle is managed on Jira, with 4th Line Support Tickets managed

		via the support & development functions on the platform.
Amazon AWS Simple Email Service (SES) (Emails)	UK	AWS SES is a UK pinned provider of cloud-based transactional and marketing email delivery, management and analytics services. These services will consist primarily of sending and delivering e-mail communications on behalf of customers to their recipients. The personal data transferred concern anyone who is a sender, recipient or copy recipient of an email which the customer instructs AWS SES to deliver and manage. Data subjects may also include individuals who are mentioned within the body of emails sent by the customer using AWS SES. The categories of personal data transferred: • Sender, recipient and copy recipient identification information (first and last name), contact information (address, telephone number (fixed and mobile), e-mail address, fax number), employment information (job title); and • Any other personal data that the Customer chooses to include within the body of an e-mail that it sends using AWS SES. The personal data transferred to AWS SES for processing is determined and controlled by the Customer in its sole discretion. As such, AWS SES has no control over the volume and sensitivity of personal data processed through its service by the Customer. Amazon SES supports TLS 1.2, TLS 1.1 and TLS 1.0 for TLS connections. By default, Amazon SES uses opportunistic TLS. This means that Amazon SES always attempts to make a secure connection to the receiving mail server. If Amazon SES can't establish a secure connection, it sends the message unencrypted.
OKTA (coming in 2024)	UK	OKTA is Staffology HR & IRIS Software identity management provider and helps companies manage and secure user authentication into applications.

Note:

Support via Salesforce – UK

Our support function uses Salesforce to provide customer ticketing, communication, live chat and query resolution management.

Information security incident management

In all critical incidents (whether relating to information security or not) are managed through the "Critical Incident Management Process", handled and coordinated by the IRIS Critical Incident Manager. Incidents are prioritised and classified as part of this process. The process outlines stakeholder communication with a focus on customer communication during an incident resolution. A post incident review is then drawn up by the software manager and / or product manager and corrective actions are logged and tracked to execution.

Information security incidents must follow this process, but in addition will be triggered by the Group Data Protection Officer. The IRIS Group Data Protection Officer will report a summary of all data protection incidents to the IRIS Information & Security Governance Group and maintain a list of learning outcomes and actions arising from incidents with the aim of ensuring Information Asset Owners follow through on those actions. This process will also be used internally for any issues discovered during development, and training is provided for staff to promote awareness of this process.

Business continuity – Information security aspects

Information Security Continuity	Description
Planning information security continuity	During adverse situations, Staffology HR have a number of secure ways to ensure the continuity work carried out.
Implementing information security	Staffology HR continues its use of the Local Data Protection Policy in the event of a BCP scenario. We also utilise the Working From Home Procedures policy and Acceptable Usage policy.
Verify, review and evaluate information security continuity	Staffology HR review all policies as often as required but no less than once per year

For additional information regarding Business continuity please visit our help centre's security section

Compliance

Compliance with legal and contractual requirements

Information Security Continuity	Description
Who is responsible for data protection compliance in your organisation?	All IRIS staff are responsible for compliance with data protection in line with IRIS policies and procedures. The Chief Information Officer (CIO) has ultimate responsibility for enforcement of policies and procedures and is supported by the governance structure described in Appendix 1 of the Group Data Protection Policy.
What processes do you have in place to ensure identification of and prompt reporting of data breaches to us and (if appropriate) the Information Commissioner's Office?	IRIS Software Group has an overarching critical incident process. The IRIS Personal Data Incident Reporting Procedure falls under that process to ensure any incident is promptly reported to the Group Data Protection Officer and assessed in line

	with the regulatory guidelines on Breach Reporting under current data protection laws. The Staffology HR Product Manager is responsible for ensuring that all staff involved in providing the service have the means to escalate incidents in line with the above corporate procedures. As your Data Processor, Staffology HR will not report personal data breaches to a regulator on your behalf. However, Staffology HR will report incidents to you without undue delay so that you can report the matter to the ICO if you believe it is necessary to do so.
Who is responsible for dealing with the response to data breaches in your organisation?	Group Data Protection Officer in consultation with the CIO.
To the extent not already set out above, what action have you taken to ensure compliance with data protection laws?	IRIS has an Information Security and Governance Group, which includes members of the Executive Committee. The Staffology HR Management Review Group leads on Staffology HR. Staffology HR has carried out a gap analysis and risk assessment in line with current data protection regulations
Do all staff receive data protection training? Please provide details.	IRIS use meta compliance to hold all Policies and procedures in relation to data protection. The compliance software tracks, records and enforces employees to: Read company policies Conduct assessments to record understanding Conduct e-learning activities in relation to data security, information security and managing incidents The group also provides onsite training to key areas to support this knowledge and understanding of the subject matter: Training - Training in place Confidentiality Training - Yes - Annually GDPR Training - Yes- Annually

Information security reviews

Information Security Reviews	Description

Compliance with security policies and standards	Local policies are reviewed as regularly as required but no less than annually. This is to ensure that all relevant standards are being met and have been implemented in full. Group level compliance reviewed annually

Data Protection – quick reference

Contact	Details
IRIS Group Data Protection Officer	Vincenzo Ardillio – dataprotection@iris.co.uk
Data protection owner for Staffology HR	Jonathan Low – Jonathan.low@iris.co.uk

Categories of personal data processed as part of the product/service provision (It is important to note that this does not represent all possibilities since Staffology HR can be highly configured)

- Name
- Address
- Email address
- Phone number
- Date of birth
- Race
- Gender
- Political opinions
- Religious beliefs
- Health data

Categories of data subjects under the product/service provision (It is important to note that this does not represent all possibilities since Staffology HR can be highly configured)

- Employees
- Students
- Volunteers
- Next of kin

Retention of data

In the context of our function as a data processor, we are required to keep customer data for the retention period agreed in the contract, which represents the customer's instructions to us. However, after the end of the provision of services relating to processing we must, at the choice of the customer, delete or return all the personal data to the customer and delete existing copies. It is up to the customer to ensure they instruct IRIS during any notice period of the end of the contract

"What happens to data when a customer terminates their contract?

Terminated customers have 30 days to extract or request a copy of their data from the Staffology system. The 30 day window begins on the date the contract has terminated and/or service provision has ended. After 30 days IRIS will permanently delete the data.

Data subject rights

The Client will remain the data controller and will have the responsibility for responding to rights requests from their employees or any other data subjects. Clients requiring assistance with a Data Subject Rights request can do so by logging a support ticket via the Staffology HRs Service Desk. A response will be received within 2 working days. Where subject matter is comprehensive or more time is required to deliver the requested data, a client will be updated with realistic timescales to satisfy their request.