SERVICE DEFINITION DOCUMENT

STAFFOLOGY BUREAU

IRIS

Contents

Staffology Bureau – G Cloud 15

The Staffology Bureau payroll software allows payroll professionals and accountants the ability to offer a comprehensive Managed Payroll service that offers:

- The end-user client to submit their permanent and temporary payroll changes via the secure cloud-based Staffology Bureau software

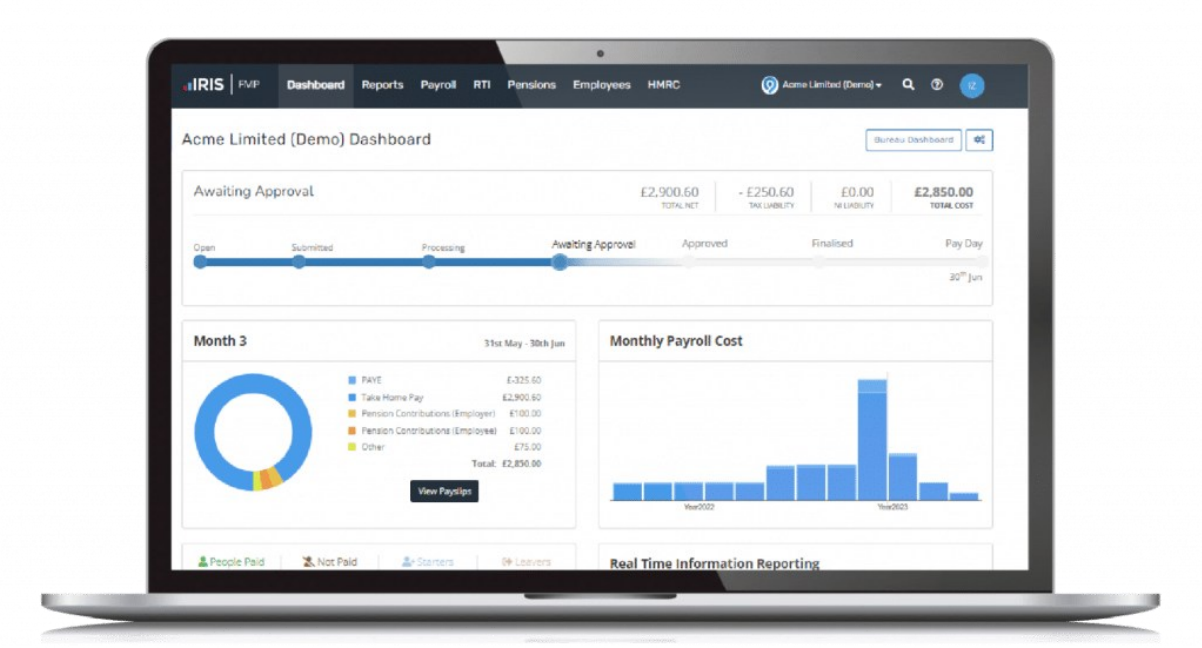
or

- A traditional payroll service using documents exchanged via Staffology Bureau is also supported

This document constitutes the solution description of bureau payroll software which is provided by Staffology by IRIS and identifies:

- The services to be provided to the Bureau Client (the Bureau)
- The scope of services that Staffology will provide and the Bureau Client (the Bureau) Responsible
- How any issues regarding the specified service will be supported

Scope of Service



The Staffology Bureau solution provides bureau payroll software, which designed to support Payroll Bureaus & Accountants with a modern cloud-based payroll experience for their colleagues and customers.

The main aim of payroll is to pay people accurately and on time. To do this, both parties must ensure the payroll is both processed accurately and checked thoroughly. Staffology Bureau software allows this process to proceed seamlessly to pay day and repeatedly to the next pay period.

What is described in the following scope of services is an illustration of how the software can be configured to run without or without customer involvement within the 'Payroll Process' and will be configured to your own and your customers' needs.

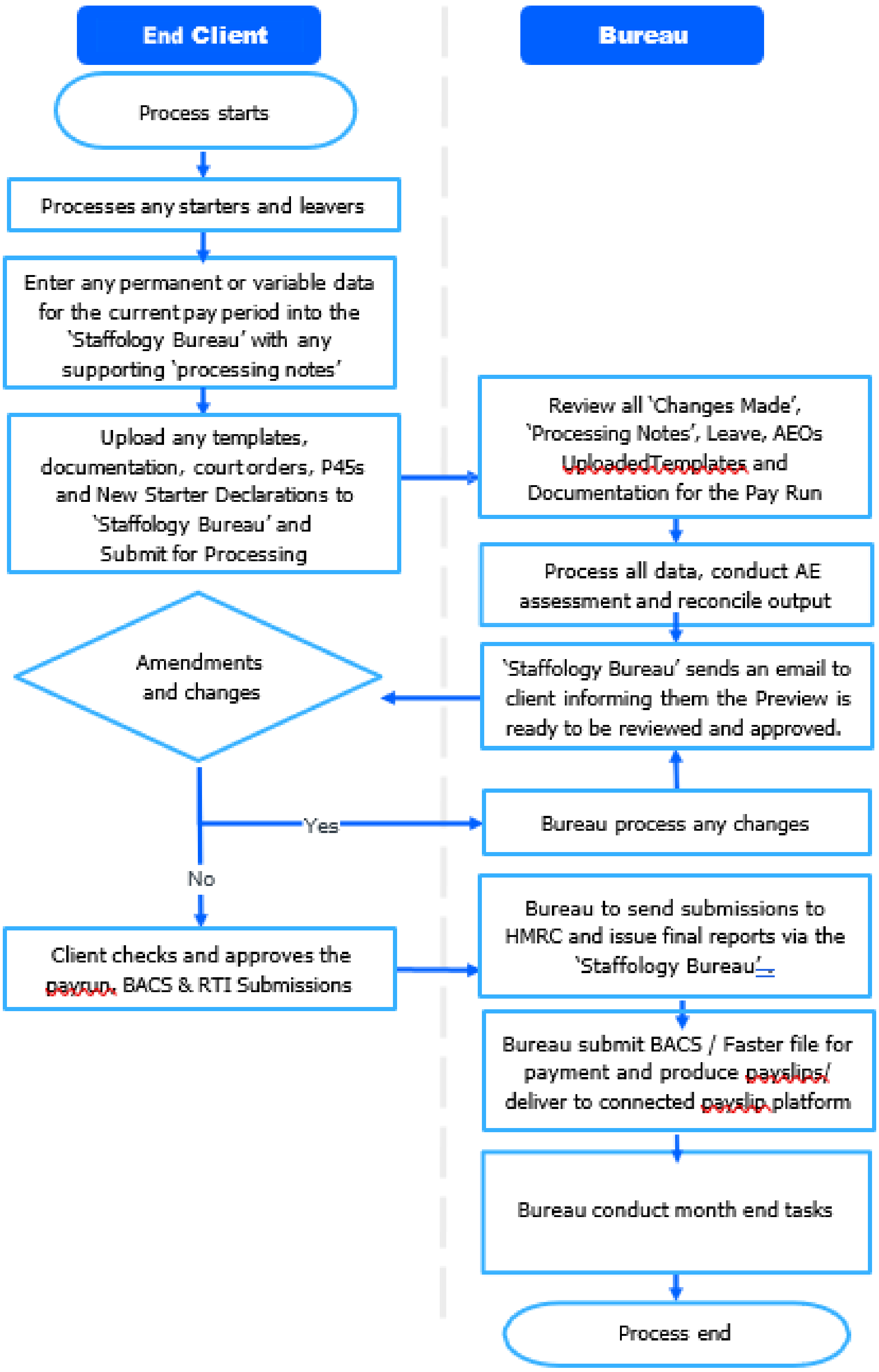
Main Payroll

Main Payroll / Staffology Bureau updates	Bureau Responsible	End Client Responsible
Download and process DPS data from HMRC (P6, P6B, P9, SL1, SL2) prior to opening a pay period	✓	
Update employee records with any permanent changes to personal information and fixed salary, payments, or deductions	✓	✓
Provide new starter information including new starter declarations and/or P45s via the New Starter Wizard	✓	✓
Provide general or statutory payment documentation via 'Staffology Bureau'		✓

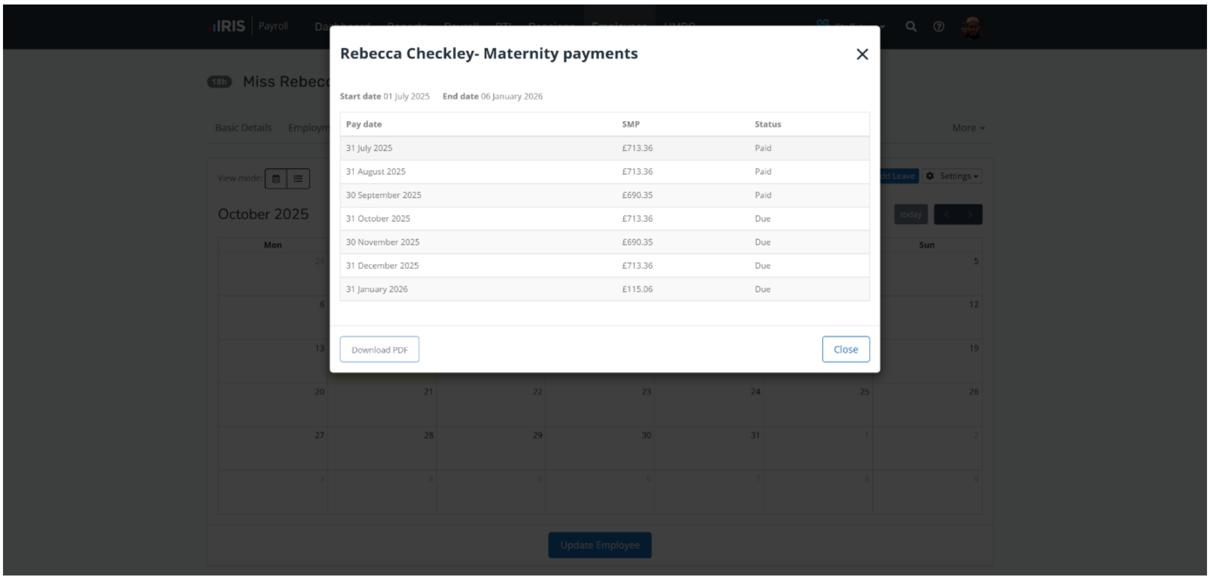
Provide the hours/salaries/additional payments/additional deductions via the 'Staffology Bureau', Bureau Template, Connector or API.	✓	✓
Provide any additional instructions relating to employees and/or the payroll as a whole via 'Processing Notes'		✓
Review the 'Changes Made' within the current Pay Period and 'Submit for Processing' in accordance with processing calendar		✓
Review all changes to the permanent and temporary data within 'Staffology Bureau'	✓	
Review All Processing Notes, Uploaded Documents, Leave and Attachment Orders	✓	
*Adding and verifying any subcontractors	✓	
Review and action any additional fixed or variable data via Processing Notes, Uploaded documents and Files	✓	
Ensure any changes to employees and/or payroll are accurate and meet current legislative requirements	✓	
Process payroll and reconcile output back to permanent and variable data supplied via 'Staffology Bureau'	✓	
Review Summary, Gross to Net, Pay slips and Pension Contributions, alongside Pay run Report Packs		✓
Check payroll and advise of any amendments		✓
Approve Pay Run, BACS and RTI submissions via 'Staffology Bureau'		✓
Finalise payroll in line with processing calendar	✓	
Provide final reporting packs	✓	
* Provide pension output files or submit pension file on client behalf via Connector, API or Manual Upload	✓	
* Send EPS, FPS, BACS or Faster Payment submissions	✓	

* Issue employee payslips / P45's / P60's. Including Delivery to MEPW, ePayslip or other Payslip distribution platforms	✓	

**If applicable*



Managed Statutory Maternity / Paternity / Adoption / Parental Leave / Shared Parental Leave



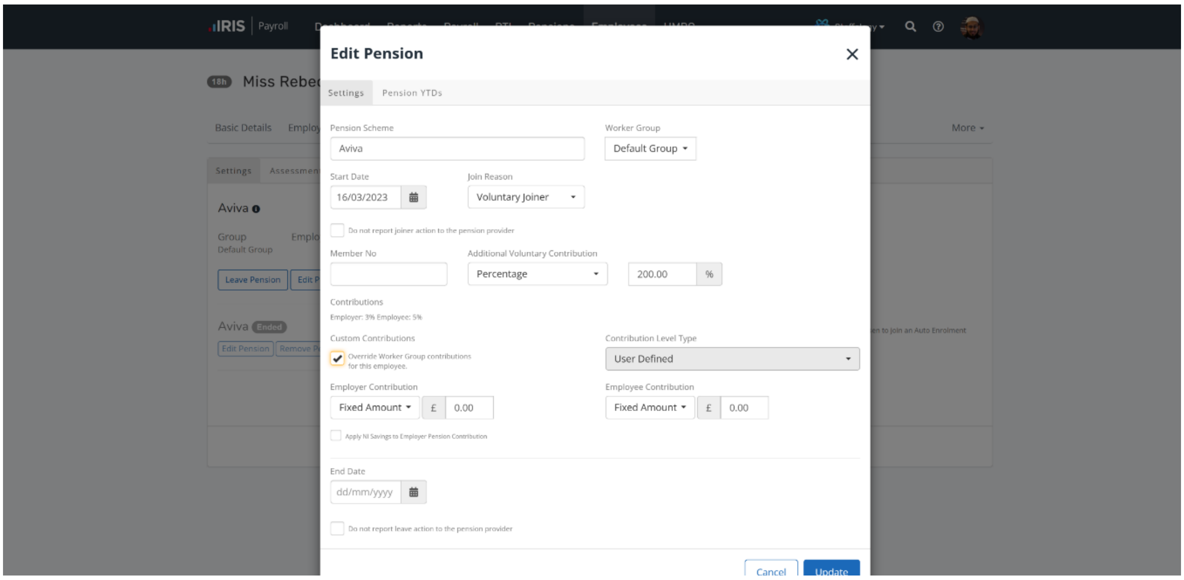
Statutory payments	**Bureau Responsible**	**End Client Responsible**
Enter leave via Leave Wizard or Processing Notes within 'Staffology Bureau' and upload any MATB1/SC3/matching certificate.		✓
Review or enter leave on employee records using dates and documentation provided, ensuring it meets the relevant legislative framework	✓	
Calculation of statutory payments processed, based on dates provided and current tax year legislation	✓	
Provide end date of statutory leave		✓

Managed SSP (Statutory sick pay) & OSS

SSP and Occupational Sickness	**Bureau Responsible**	**End Client Responsible**
Enter leave via Leave Wizard or Processing Notes within 'Staffology Bureau' and upload any supporting documentation.		✓
Review or Enter Leave on employee records using dates and documentation provided, ensuring it meets the relevant legislative framework	✓	
Calculate SSP due based on employee shift pattern	✓	
If employee is not entitled to SSP, inform client that SSP1 needs to be produced	✓	

Issue SSP1 form to employee		✓
Calculate occupational sick payments and supply value as variable payment and deduction		✓

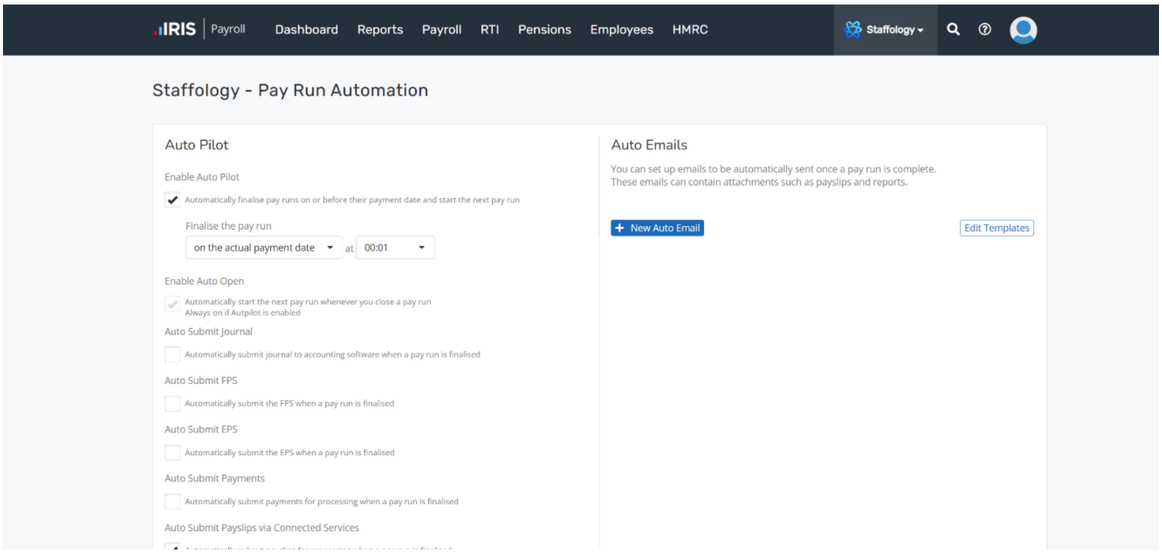
Managed Auto Enrolment



Auto Enrolment	Bureau Responsible	End Client Responsible
Assess each employee’s AE status	✓	
Decide whether the pension is to be salary sacrifice or a net pay arrangement		✓
Make appropriate pension deductions	✓	
Publish AE communications	✓	
*Produce pension upload file	✓	
*Upload data to pensions provider manually or via Connector or API	✓	

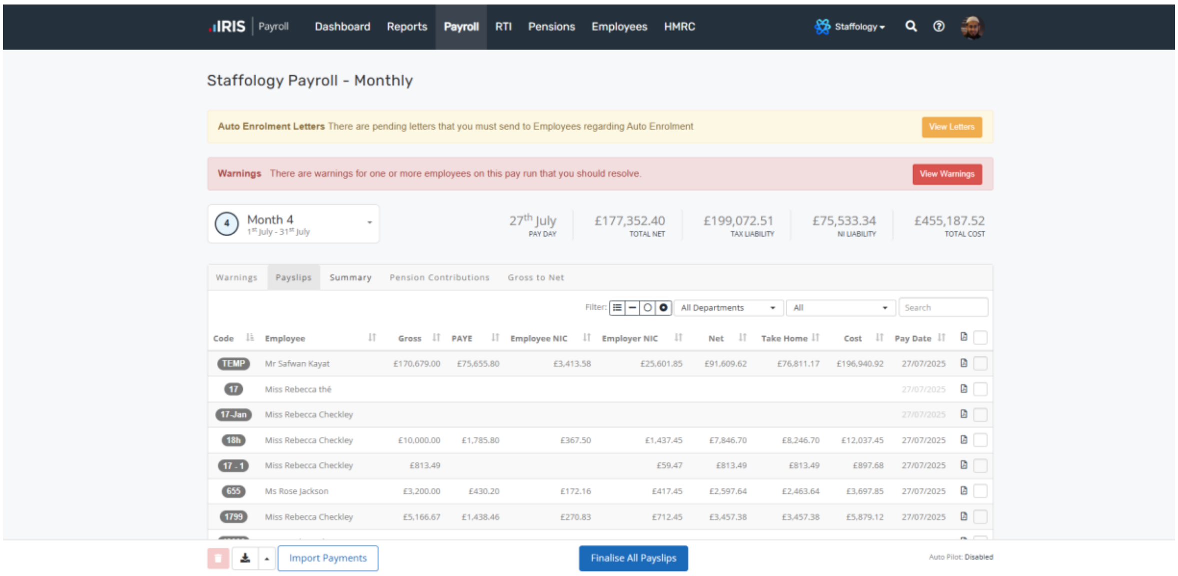
If applicable

Pay Run Automation



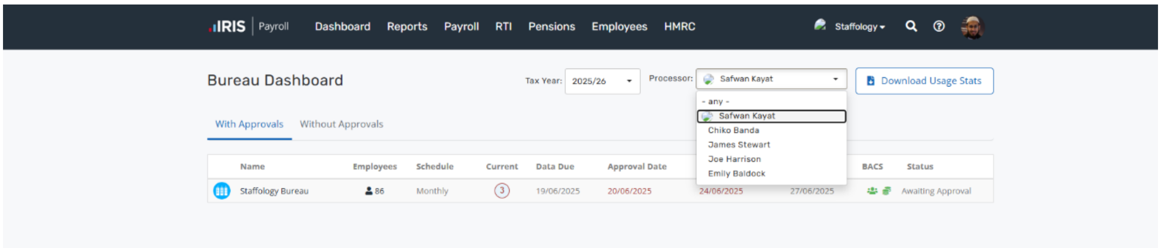
Pay Run Automation	**Bureau Responsible**	**End Client Responsible**
Enable Auto Pilot - automatically finalise pay runs on or before their payment date and start the next pay run	✓	
Enable Auto Open - automatically start the next Pay Run whenever you close a pay run	✓	
Enable Auto Journal Submission – automatically submit journal to accounting software when a pay run is finalised	✓	
Auto Submit FPS – automatically submit the FPS when the Pay Run is finalised	✓	
Auto Submit Payments – automatically submit payments for processing when the pay run is finalised	✓	
Auto Emails – configure emails to automatically send once a Pay Run is complete including reports & pay slips (password protected)	✓	

Pay Run Warnings



Pay Run Automation	**Bureau Responsible**	**End Client Responsible**
Configure Pay Run Warnings as per Bureau & Client requirements: - Employees with No Bank Details Provided - Missing or Invalid Details for FPS Submission - Employee on Invalid NI Letter Table - Employee is earning below National Minimum Wage - Employee is paid above Gross or Net Pay Threshold - Employee is receipt of Tax Refund - Target Net Pay Amount could not be reached	✓	
Resolve Warnings to allow the accurate & timely processing of payroll to pay schedule	✓	✓

User Management



User Management	**Bureau Responsible**	**End Client Responsible**
Add, Edit & Delete Bureau Users and manage their relevant permission levels within Staffology Bureau	✓	
Provide details of initial Authorised Client Users to the Bureau for them to be set-up as Client Users on Staffology Bureau		✓
Add, Edit & Delete Client Users and manage their relevant permission levels within Staffology Bureau	✓	✓
Assign Bureau or Client Users to Employers to allow them to manage the payroll process	✓	

Pay & Nominal Code Management

User Management	**Bureau Responsible**	**End Client Responsible**
Bureau to have reviewed default system Pay Codes and set-up any Bureau Bespoke Pay Codes	✓	
Client to provide Bureau with detailed payroll information to allow for the configuration bespoke Pay Codes		✓
Bureau to assign any default or bespoke Pay Codes to Employer where applicable	✓	✓
Bureau to ‘Import’ any Bespoke Pay Codes where applicable to save time on configuration	✓	
Client to provide Bureau with detailed nominals to allow for the configuration of Nominal Codes to Pay Codes		✓
Bureau to map any default system or bespoke Pay Codes to ‘Nominal Codes’ provided via the Client	✓	

Department Management

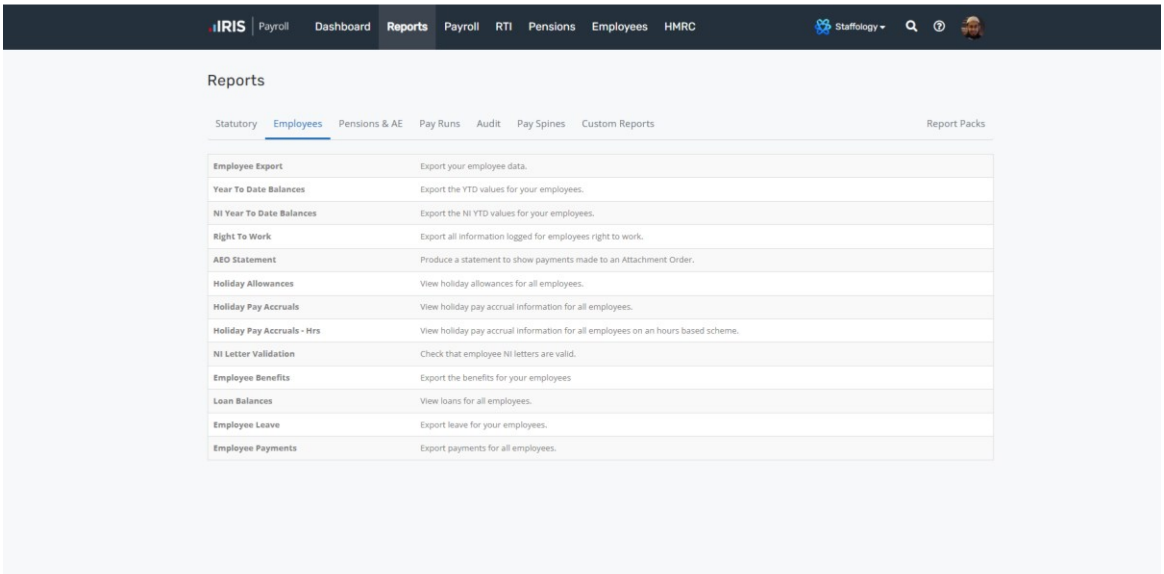
Department Management	Bureau Responsible	End Client Responsible
Client to provide Bureau with detailed information on Departments, employees within Departments and any related 'Accounting Codes'		✓
Bureau to set-up Departments within the initial implementation of the Employer	✓	
Bureau to import Employees against departments within the implementation of the Employer	✓	
Client to maintain the departments and employees within departments within the payroll process		✓

Working Pattern Management

Working Pattern Management	Bureau Responsible	End Client Responsible
Client to provide Bureau with detailed information on 'Working Patterns' and treatment of related 'Bank Holiday's and 'Pro Rata Rules'		✓
Bureau to set up Working Patterns within the initial implementation of the Employer	✓	
Bureau to import Employees against Working Patterns within the implementation of the Employer	✓	
Client & Bureau to maintain the 'Working Patterns' and employees within 'Working Patterns' within the payroll process	✓	✓

Standard Output Reports

This section relates to the reports you receive as part of the service. We have over 30 standard reports to choose from depending on your requirements and that of your individual customers. These reports can be bundled up into 'Reporting Packs and provided to customers via the portal or send via password protected emails. When viewed online, some of these reports allow users to select a prior pay period for comparison to spot for changes / anomalies.

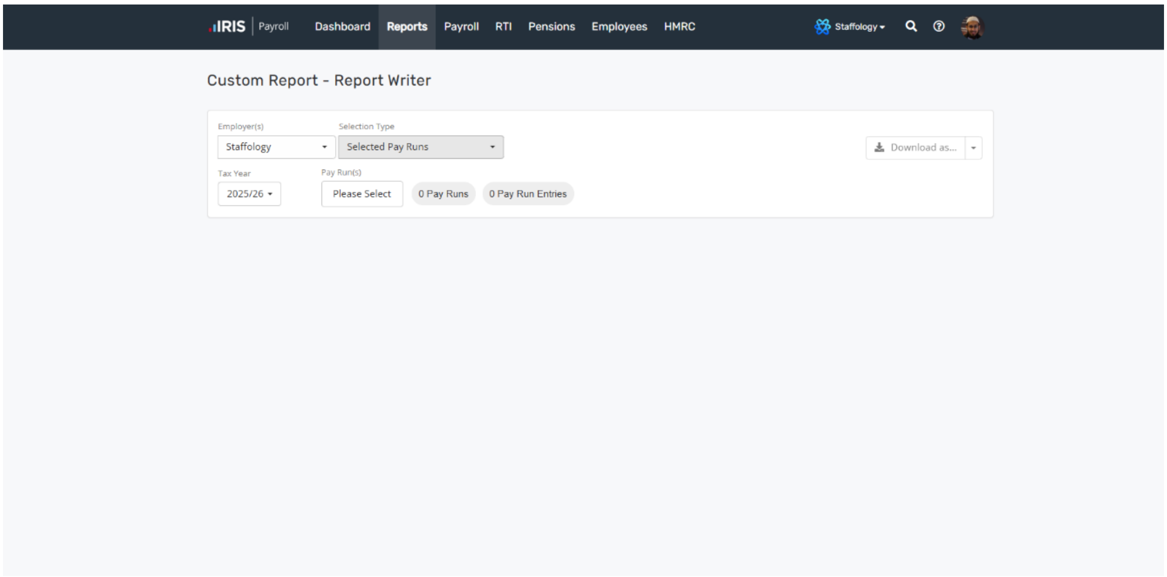


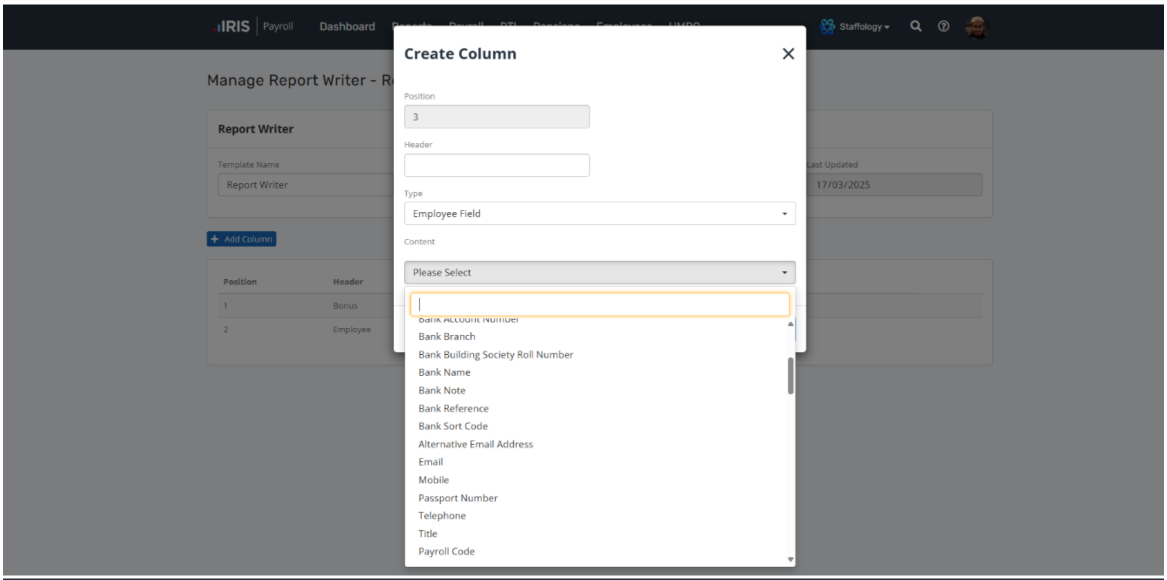
Most reports are available in a variety of formats such as PDF, CSV and Excel

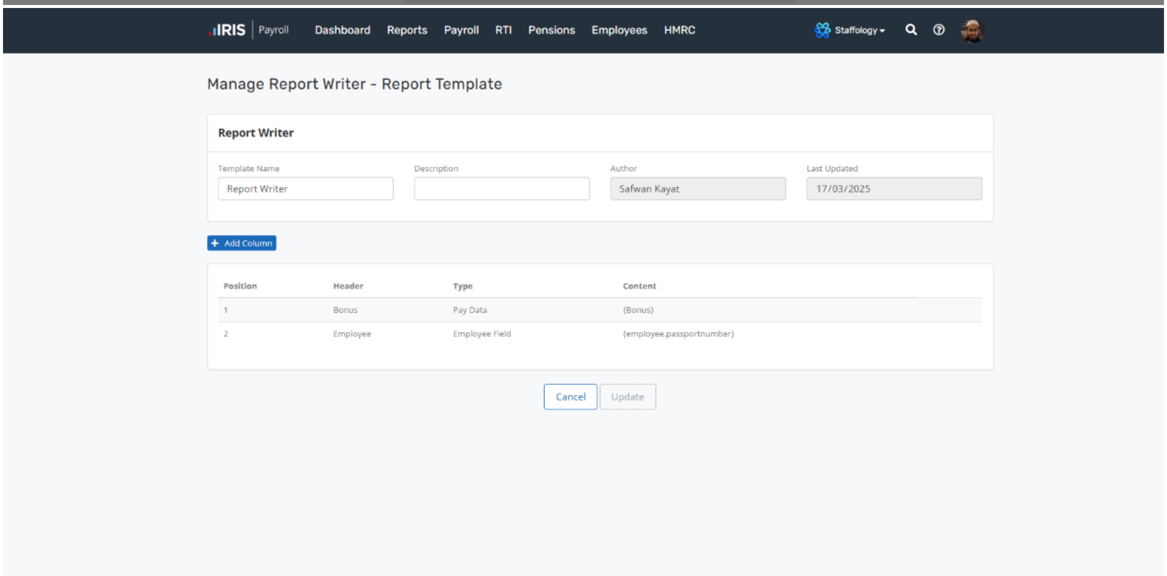
Payroll Reports	**Description**
P11	Generate a P11 to summarize pay and deductions to date.
P11 Detailed	Generate a detailed P11 for a breakdown of pay & statutory deductions.
P11D	Generate a P11D to detail Benefits and Expenses.
P30	Generate a P30 to summarize your HMRC liabilities.
P32	Generate a P32 to view the details of your HMRC liabilities.
P45	Generate P45s for employees that are leaving.
P60	Generate P60s to give to your employees at the end of a tax year.
Apprenticeship Levy	Generate a report showing your Apprenticeship Levy calculation breakdown per period.
Payroll Analysis	Analyse payroll by employee across multiple periods.
Required Payments	Generate a detailed P11 for a breakdown of pay & statutory deductions.
Payrun Journal	View the journal entry required for a Pay run.

Gross to Net	Compare your employees' gross pay with their net pay for one or more pay periods.
Variance Report	Compare one period (or range) to another period (or range).
Cost Analysis	Analyse payroll costs and statistics for one or multiple periods.
Cost Of Employment	Analyse payroll costs per employee across one or many periods.
Full Summary Of Pay	Get a detailed breakdown of the pay and deductions made to each Pay Code in a pay run.
Hourly Pay	Summary of hourly pay for one or more pay periods.
Statutory Pay	Produce a report detailing statutory payments made on one or more pay runs.
Furlough Claim Report	Generate a report to reclaim pay for furloughed employees.
NI Letter Validation	Check that employee NI letters are valid.
Year to Date Balances	Export the Year-to-Date values for your employees.
Tax Code Changes	Changes of Employee Tax Codes over a period.
Attachment Orders	View attachment of earnings orders deductions for one or multiple periods
AE Assessments	View the Auto Enrolment status of your employees and when they were last assessed.
Pension Contributions	View the contributions made to each of your schemes.
Member Statement	View Employees being enrolled into a pension.
Employee Export	Export your employee data.
NI Year to Date Balances	Export the NI YTD values for your employees
Right To Work	Export all information logged for employees right to work.
AEO Statement	Produce a statement to show payments made to an Attachment Order.
Holiday Allowances	View holiday allowances for all employees.
Holiday Pay Accruals	View holiday pay accrual information for all employees.
Employee Benefits	Export Benefits for your employees

Bespoke Report Writer







Glossary of Terms and Definitions

Statutory Terms		
AE	Auto Enrolment	Under the Pensions Act 2008, every employer in the UK must put certain staff into a pension scheme and contribute towards it. This is called 'automatic enrolment'.
AEO	Attachment of Earnings	Payment of debts by direct deduction from the debtor's earnings, under a court order.
CIS	Construction Industry Scheme	Bureau Clients must register as a contractor with the Construction Industry Scheme (CIS) if: - The Bureau Client pays subcontractors to do construction work - The Bureau Clients' business doesn't do construction work but usually spend more than £1 million a year on construction
Class 1A	Class 1A National Insurance	As an employer, we must pay Class 1A National Insurance on work benefits given to employees, e.g., a company mobile phone.
CMS	Child Maintenance Service	Child maintenance is financial support towards a child's everyday living costs when separated from the other parent.
CSA	Child Support Agency	Child maintenance is financial support towards a child's everyday living costs when separated from the other parent.
DEA	Direct Earnings Attachment	As an employer, you may be asked to deduct any benefit overpayment an employee owes the Department for Work and Pensions (DWP) from their pay. This is called Direct Earnings Attachment.
EDI	Electronic Data Interchange	Allow a secure electronic exchange of PAYE information between employers and HMRC.
EPS	Employer Payment Summary (RTI process)	An employer must complete and submit an FPS whenever they make a payment to an employee. These form part of the (RTI) Process.
EYU	Earlier Year Update (RTI process)	Earlier Year Update forms part of (RTI) Process - If pay/deductions for previous tax years have been reported incorrectly, an Earlier Year Update (EYU) needs to be submitted showing difference between what was originally reported and the correct figure.
FPS	Full Payment Submission (RTI process)	Full Payment Submission (RTI process) - The FPS is the submission that must be made to HMRC each time an employee has been paid, with any new starters, process employees paid infrequently, and process leavers.
HMRC	HM Revenue & Customs	Her Majesty's Revenue and Customs (HM Revenue and Customs or HMRC) is a non-ministerial department of the UK Government responsible for the collection of taxes, the payment of some forms of state support, and the administration of other regulatory regimes including the national minimum wage.
KIT	Keeping in Touch	Employees can work up to 10 days during their maternity, adoption or additional paternity leave. These days are called 'keeping in touch days'. Keeping in touch days is optional - both the employee and employer need to agree to them.
PAYE	Pay as You Earn	Tax payment method in which an employer is required by law to deduct income tax (and national insurance, if applicable) from an employee's taxable wages or salary.
P32	HRMC form containing the	HRMC form containing the Employer Payment Record - details a record of total payments and deductions made for each pay period.

	Employer Payment Record details	
RTI	Real Time Information	An electronic way of submitting payroll information to the HMRC in real time.
SAP	Statutory Adoption Pay	It is a weekly payment from an employer to help take time off work when someone adopts a child. To qualify for Statutory Adoption Pay the person must have been: matched with a child for adoption by an adoption agency employed by their present employer without a break for at least 26 weeks up to and including the week the adoption agency told informed that they had been matched with a child for adoption earning an average of at least £112 a week (before tax).
SMP	Statutory Maternity Pay	Is there to help Eligible employees to take time off work both before and after the birth of their baby, this is a weekly payment from the employer.
SPP	Statutory Paternity Pay	Eligible employees may be entitled to Statutory Paternity Pay SPP, sometimes referred to as Ordinary Statutory Paternity Pay when their wife, partner or civil partner gives birth or adopts a child.
SSP	Statutory Sick Pay	Statutory Sick Pay - Employees unable to work because their ill may be able to claim Statutory Sick Pay. It is paid for by the employer and can be paid for up to 28 weeks.

Statutory Forms	
MATB1	The Maternity Certificate (MAT B1) enables a pregnant woman to claim: - Statutory Maternity Pay (SMP) from her employer - Maternity Allowance (MA) from Job Centre Plus
NVREQ	National Insurance number verification request
NVREP	National Insurance number verification reply
P6	Individual in-year tax code changes
P6B	Individual budget tax code changes
P9	Tax code to use for an employee
SL1	Start making student loan deductions
SL2	Stop making student loan deductions
SSP1	Statutory Sick Pay Form
GL	General ledger
P11D	An employer may provide an employee with a copy of their P11D if they used it to tell HM Revenue and Customs (HMRC) about their 'benefits in kind' (e.g. company cars or interest- free loans).
P46	When a car is provided for private use to an employee
P45	An employer will provide a P45 when the employee stops working for them
P60	A P60 shows the tax an employee has paid on their salary in the tax year (6 April to 5 April)

Information Security Assurance Statement

The purpose of this information security assurance statement is to provide customers of Staffology Payroll by IRIS with transparency as to the security and personal data compliance of this product and associated products (MyePayWindow) 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 Payroll as a thoroughly secure software and service provider.

Description of the data processing carried out by Staffology Payroll

Staffology Payroll Is a payroll software under the IRIS family. We offer end-to-end payroll processing functions using the latest in secure cloud hosted technology, along with real-time payroll calculations and connectivity via APIs & pre-built connectors.

The objective of the software is to:

- **Support Compliance:** Keep your business ahead of regulatory change with a simple to use and comprehensive solution that mitigates any risks.

- **Drive Productivity:** Automate both mundane and complex operational tasks, whilst also providing new data and insights to drive business success, saving you time and money.

- **Improve Engagement:** Build a culture of employee engagement by providing a user-friendly experience that unifies services and software and eliminates duplication

Staffology Payroll platform provides various types of payroll related services such as employee record maintenance, payroll calculations, HMRC reporting, accounts journal output, BACS processing to employees and 3rd parties, pay slip distribution and payroll queries.

The Platform offers optional API connectivity with applications such as accounting. HR, Time & Attendance. We have robust data security measures in place to ensure that our customer's data is protected in every way.

Statement of Assurance

Staffology Payroll will ensure that:

- We will put in place measures to protect customer information from a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- We will meet our regulatory and legislative requirements.
- We will produce, maintain and test Business Continuity plans.
- We will provide information security training to all our staff.
- We will report and investigate information incidents (whether actual or suspected), in line with our Incident reporting procedure.
- 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 Payroll Organisational Security

Staffology Payroll is committed to fulfilling its obligations under the Data Protection Act 2018, General Data Protection and Regulation (GDPR – EU law) and any associated privacy legislation that affects how Staffology Payroll uses or handles personal data. The statement of assurance is provided to assure our customers and staff of our commitment to data security.

Additionally, this document sets out the Staffology Payroll Statement of Data Protection Policy, and this document sets out how responsibility for data protection and information security is designated. It includes high-level descriptions of the procedures in place that must be followed to ensure personal data is handled in a responsible, accountable and secure manner.

Staffology Payroll will use personal data legally and securely regardless of the method by which it is collected, recorded and used and whether we hold it within our products, on a Group or third-party network or device, in filing systems, on paper, or recorded on other material such as audio or visual media.

Staffology Payroll regards the proper management of personal data as crucial to the success of our business. Observing good data protection practice plays a huge role in maintaining customer confidence. We ensure that Staffology Payroll respects privacy and treats personal data lawfully and correctly.

Supporting accreditations held by Staffology Payroll are:

- HMRC-Recognised Payroll Software
- ISO 27001
- ISO 9001
- Cyber Essentials
- G-Cloud Framework

Our support function also holds the following accreditations:

- ISO 9001 (Support Function)
- ISO 27001 (Support Function)

We employ the use of cloud-based technology that houses personal data in UK Data Centres, that uses world-class security protocols to ensure security compliance. The data that is stored by Azure is protected or regulated under:

- *ISO 27001*
- *ISO 27018*
- *SOC 1*
- *SOC 2*
- *SOC3*
- *FedRAMP*
- *HITRUST*
- *MTCS*
- *IRAP*
- *ENS*

Organisational Security at IRIS Group Level

Data protection and information security at IRIS Software Group is controlled by the IRIS Information Security and Governance Forum. This forum 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
- Other key security leads within the company

The Information Security and Governance Forum approve 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 Payroll

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

Department	**Designation**
Product	Senior Product Director – Payroll & Managed Services
HCM Engineering	Engineering Director, Staffology
Product	Product Manager, Staffology
HCM Engineering	Software Engineering Manager, Staffology
Customer Service/Support	Senior Manager, Customer Services
Professional Services	Professional Services Director
Finance and Accounts	VP, Financial Controller
Sales Order Processing	Director, Revenue Operations
Central Compliance	Data Protection Officer – Group

The Staffology Payroll 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 Payroll.

Measures are “appropriate” if they have been identified through risk assessment.
Date of last Staffology Payroll risk assessment review: 28th February 2025.

The Staffology Payroll 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 Payroll 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 Payroll's IT systems and for keeping systems reasonably up to date.

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

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

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

Staffology Support staff could have access to your data in order to fulfil the Support aspect of the Payroll Solution

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 is held with Staffology Payroll 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 requires the completion of corporate policy training and the subsequent testing of this knowledge through the MetaCompliance 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 re-reviewed and amended to ensure stricter compliance moving forwards. Staffology Payroll 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 discipline, employment is terminated as set out in the terms of the procedure.

Termination 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 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 Payroll, 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 have 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 Payroll 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 out 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 on a basis consistent with an individual's job/role responsibilities. For Staffology Payroll 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 both Single Sign On (SSO) and Multi-factor Authentication (MFA) with Staffology Payroll 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.

Password and Authentication Policy

This policy describes the authentication requirements for accessing internal computers and networks and includes those working in-house as well as those connecting remotely. Every person, organisation or device connected to internal IT resources and networks must be authenticated as a valid user before gaining access to IRIS's computer systems, networks and information resources.

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

Staffology Payroll Physical and Environmental Security

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

Physical entry controls - Entry to the site is restricted to key fob or keypad 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 Payroll has a robust business continuity plan, however we also place 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 can move the entire site remote or transfer ownership to a satellite office at a moment's notice.

IRIS Group have invested heavily in 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 always escorted 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.

Equipment

Equipment	**Description**
Equipment sitting and protection	Access to critical computing resources or infrastructure is physically restricted to authorised personnel with access controlled by keys, swipe cards or a keypad 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	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 Payroll 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 required to log off from sessions and ensure any paper is securely disposed of.
Clear desk and screen policy	Staffology Payroll went 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 Payroll 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 Payroll 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, and 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 Payroll 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	The backup of all processing server systems falls under the remit of the Group IT Director. All data is backed up at least nightly and transmitted to a secure UK-based cloud back-up location. Restoration tests are made and documented on a regular basis, not less than annually.
Event logging	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 Payroll Management.
Protection of log information	Log information and Audit trails are managed at Group IT level in line with outlined roles and responsibilities to prevent tampering of data. Ona software product level, these controls have been locked at development stage, no user has the ability to manipulate information held within.

Clock synchronisation	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 reviews 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.

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 people 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 non-disclosure agreements	As required, Staffology Payroll 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.

How we transmit confidential information to customers

Dependent on the service provided, Staffology Payroll utilises an inbuilt proprietary secure document sharing function (Processing Notes') to transmit client personal data between client and Staffology Payroll, we also send password protected documents issued by email direct from the software product. Dependent on the service the use of email is minimised for queries and all personal identifiable data is removed from the contents of email transactions in direct reply to a query. All employees receive audited training against this requirement.

Information transfer policies and procedures – Staffology Payroll clearly outlines the procedures within the IRIS Data Protection Policy held at local level for the teams. It is meticulous in the process that must be followed to prevent risk occurring when transferring information between Staffology Payroll and Client.

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 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.

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 support agents, 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

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 security and data protection teams ensure potential suppliers are subject to due diligence in line with data protection laws and security standards.

List of third parties and sub-processors involved in Staffology Payroll processing customer data 6th November 2023.

IRIS Group Entities

IRIS Group Entities	Description
IRIS KPO India	Staffology Payroll regularly use all of our support centres including our Indian off-shore function in the provision of our support services. IRIS KPO use our internal secure IRIS VPN connection alongside the security architecture Azure provides to process data within UK Servers. A detailed risk assessment is carried out annually to ensure continued process review of security requirements. A full Customer Assurance document is also available on request.

External Suppliers which are Data Processors

External Data Processors	Data Location	Description
Microsoft Azure Hosting	UK & ROI	Payroll Software and client data is held in a Microsoft Azure hosted environment. All security protocols and accreditations are mentioned previously within this document.
Microsoft Azure Hosting	UK	IRIS EVC Connector service, to allow employee earning income verification via 3rd party suppliers such as Equifax & Experian. work report
Amazon Web Services	UK & US	AWS technologies are leveraged to provide automations and enhancements to customer services – including query resolution/management/communications
Microsoft Azure DevOps	UK	Staffology Payrolls development lifecycle is managed on Microsoft Azure Dev Ops, with 4th Line Support Tickets managed via the support & development functions on the platform.

Fresh Desk	EEA	Our support function uses Fresh Desk to provide customer ticketing, communication and query resolution management.
Sales Cloud via Salesforce	UK	Our support function uses Sales Cloud to provide customer ticketing, communication, live chat and query resolution management.
Send Grid	US	SendGrid is a US provider of cloud-based transactional and marketing email delivery, management and analytics services. Where customers use their own SMTP relay to send emails from Staffology Payroll this sub- processor isn't used.
OKTA	UK	OKTA is Staffology Payroll & IRIS Software identity management provider and helps companies manage and secure user authentication into applications.
Cybage PTY Limited	India	3rd party software development partner who support us with DevOps processes for Staffology Payroll.
Abstract Group Ltd	UK & India	3rd party software development partner who support us with DevOps processes for Staffology Payroll.

Information Security Incident Management

Management of information security incidents and improvements

In all instances, any desktop or cloud payroll 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

Information Security Continuity	Description
Planning information security continuity	During adverse situations, Staffology Payroll have a number of secure ways to ensure the continuity work carried out.
Implementing information security	Staffology Payroll 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 Payroll review all policies as often as required but no less than once per year.

Redundancies

Redundancies	Description
Availability of information processing facilities	All systems and data have been loaded into secure cloud based environments (Azure) to ensure continuity.

Compliance

Legal and Contractual Requirements	Description
Identification of legislation and contractual requirements applicable to Staffology Payroll	Within the scope of the role performed, processors, managers and software provisions will defer to HMRC Regulations for PAYE, attachment of earnings documentations provided by courts and terms and conditions with client. Staffology Payroll makes every effort reasonable to inform its clients of any major changes to legislation within these areas.
Protection of records	Covered in the Business Continuity Plan Document
Privacy and protection of personally identifiable information	Covered within Staffology Payroll's Data Protection Policy both at local and group level.

Regulation of Cryptographic Controls	Staffology Payroll has been developed using market leading encryption methods. These fall well inside the scope of existing legislation and additional security measures such as MFA have been built in to the existing framework. 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.

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.

Categories of personal data processed as part of the Staffology Payroll provision:

- Trade Union Membership – identifiable through deductions made to employees
- Information relating to criminal convictions and offences – identifiable though court order fines processed through payroll

Categories of data subjects under the Staffology Payroll provision:

- Employees – identifiable through payroll processing
- Trainees – identifiable through payroll processing (apprenticeships)
- Next of Kin – identifiable on rare occasion where beneficiary payment needs to be made through payroll
- Location of personal data processing

All personal data is held within payroll software databases and on electronic documents from client communicating this data to Staffology Payroll. In all instances, information is held on secured network drives held in the UK and only accessible by those authorised to access it.

On occasion, Staffology Payroll may use IRIS Support employees in India to resolve individual support queries and that access is granted by the customer & automatically removed 30 days after access is granted. . All relevant security requirements have been addressed and further information including their version of the Customer Assurance document is available on request. A full risk assessment is carried out annually to ensure that client data is always protected.

Retention of data

The Staffology Payroll platform will retain payroll data indefinitely (or until removed by an admin user) and will delete it in accordance of Staffology Payrolls terms & conditions, with appropriate notifications prior to deletion.

The IRIS myePayWIndow cloud service retains data as follows:

- Payslips, P60s, P11Ds, P45s, CIS statements are retained for at least 12 months and for the duration of processing of the client's data on myePayWindow
- Auto enrolment letters are retained for 12 months after which they are auto deleted

- Any documents uploaded to myePayWindow will be available for at least 3 months and the Website will warn you in advance of any deletions so that you can download information in advance.
- If an Employee leaves an Employer their data and access to it will be maintained for 15 months, during which information can be downloaded as required. After 15 months their account will be disabled and after a further 1 month their data will be anonymised.
- Clients who have not accessed or uploaded new data in the preceding 12 months will be deemed to be no longer using the IRIS myePayWindow service and will have their accounts blocked and their data will be anonymised after a further 3 months.

We may use aggregated information for the purpose of monitoring use of the Website. Such aggregated information may be provided to third parties. These statistics will not include information which can be used to identify any individual, Client Company or client entity or the nature of its employment or business.
For the avoidance of doubt, we shall not use any personal data held on the Website for any marketing purposes.

IRIS EVC Connector used with Staffology Payroll retains data as follows: (See EVC details here)

For the contracted or agreed duration of processing using IRIS software, employee pay details are uploaded per period to IRIS's MS Azure EVC connector environment sufficient to support income verification for between 3 to 12 months prior employment. Data is auto deleted after a rolling 15 months

If an Employee leaves their employer, their data will be auto deleted after 15 months
Each Employer's opt-in/out status is retained on IRIS's EVC connector so that Employees of participating employers can be processed accordingly or informed to verify their income by other means.

Data is permanently erased from IRIS's EVC connector when Employees or Employers opt out the service from Staffology Payroll.

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 email to the Staffology Payrolls inbox. 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.

Available Appendices

Details	
Azure	https://azure.microsoft.com/en-gb/explore/trusted- cloud/compliance
Staffology Due Diligence	Available on Request
Staffology Payroll Group Data Protection Statement	Available on Request
IRIS Working from Home Policy	Available on Request

IRIS Group Acceptable Use Policy	Available on Request
IRIS Personal Data Incident Reporting and Investigation Procedure	Available on Request
Employee Verification Check (EVC) Customer Informational Security Statement	Available on Request

Implementation

Staffology Payroll Bureau– End to End Process

Presales
Customers can review details on the Staffology Website and arrange a meeting with one of our presales consultants who will demo the system and answer any questions. Or they can sign up for a system for free and trial the use of it.

Sales
When the customer wishes to purchase the system, they will be in contact with one of the sales consultants who will explain costs and arrange the Direct Debit Mandate to be completed. This is then passed onto SOP.

Sales Order Processing
When a sale is created it is passed to the SOP team to check all the information is correct in our Salesforce system. Once all checks are completed a Delivery Engagement is created and this is passed to the Professional Services Team.

Booking of Sessions
The Project Coordinator will then contact the customer to book in the consultation sessions. The details of each session are provided later in this document.

Data Imports
This service is something we can assist with. You can either import data using templates which we can provide. Or if you are moving your payroll from an IRIS Product, we can look at how we can export the data out of your system in the easiest method to populate these templates and import them into Staffology.

If you have Staffology HR the 2 systems can be linked via an API and this integration setup is through an additional service.

Teams Invites
The product consultant will send out Teams invites to the customer for each of the sessions at least 2 weeks in advance of them occurring. They will provide a course outline with each of these invites detailing what is to be covered.

Training sessions
The training sessions will be online and in a one-to-one capacity with the customer and the consultant. During the session they will access the customers system and share their screen to show sections and explain what is required. At other times the customer may be asked to share their screen and drive the system to show their knowledge and understanding.

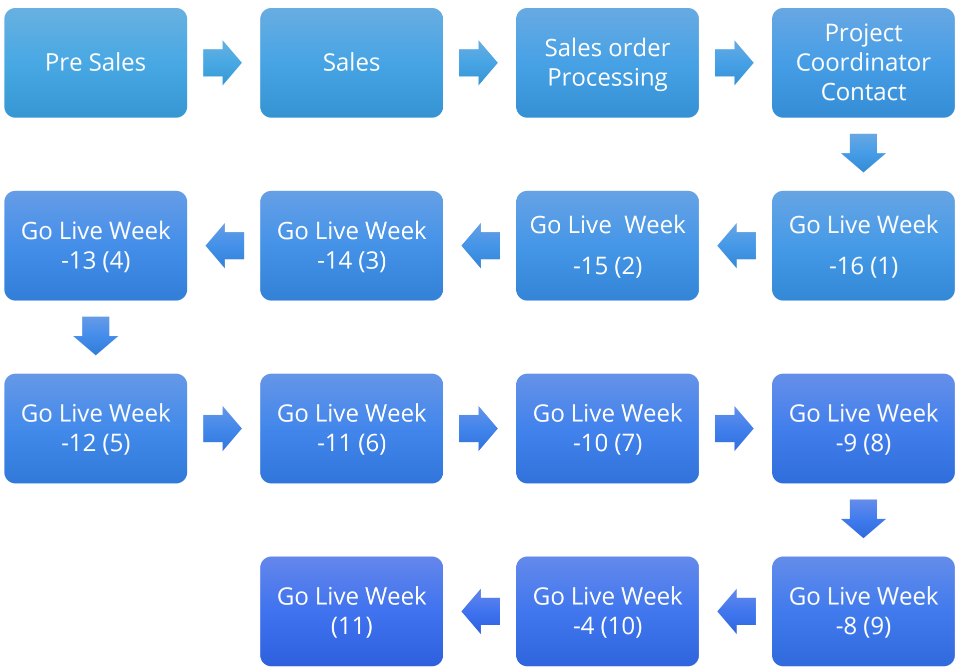
Staffology Payroll Bureau Training Sessions

The sessions are below. Please note that these sessions will be spread out at a pace which suits the customer and with advice from the consultant depending on the size and make up of your organisation.

Branding	Altering the appearance of the system (1)	
	Adding URL's and Email settings (2)	3.75h
Setup Or Migration	Adding Company details for 5 companies (3)	
	Training on import templates (4)	3.75h
Data Import	Process for Importing data (5)	
	Importing Prepared data (6)	3.75h
Training	How to use the system (7)	3.75h
	How your customers use the employer portal (8)	3.75h
Parallel Run	(9)	7.5h
Parallel Run 2	(10)	7.5h
Go Live Support	(11)	7.5h

Potential Project Plan

We advise that each session has at least a week between them as there will be additional work which the customer requires to complete between sessions. However, this could be completed quicker if required.



Implementation Complete
Once the implementation is complete the customer will be fully handed over to our support team. Should they have any problems with their system they can log a ticket and a support consultant will contact the customer to resolve.

Training after Implementation or Changes to Account
If the customer wants to make changes to their Licence numbers or account level they can contact their account manager. If they wish to purchase additional training for after implementation, perhaps they have new employees who need training, again they should contact their Account Manager to purchase this time.

Ongoing Support

This is not a legal document; the scope of this document is to guide customers on how their engagement with IRIS Service will work. Target response and resolution times quoted here may vary from some customer contracts.

Staffology's support for any technical support is Monday to Friday between 9:00am and 5.00pm (UK Time) excluding English bank holidays.

Staffology Payroll Help Hub https://help.staffology.co.uk/payroll	**IRIS Community Help Hub** https://help.iris.co.uk/servicecommunity
IRIS Service Community htps://www.iris.co.uk/iriscommunity	**IRIS Service Community - Forgotten password** https://www.iris.co.uk/communityforgotpassword

What target response and resolution timescales should I expect?
• P1. Response = 30 mins, Resolve = 4 hours
• P2. Response = 60 mins, Resolve = 8 hours
• P3. Response = 4 hours, Resolve = 10 days
• P4. Response = 72 hours, Resolve = 90 days
• P5. = No SLA

Our SLA clock is paused when we are waiting for a customer response. e.g., Case status = On Hold. You can see the case status in the community. (Service Cloud / IRIS Community only). Unscheduled maintenance will only be carried out with 48 hours' notice and receipt of confirmation from the customer. For the purposes of SLAs Unscheduled maintenance will count as Scheduled maintenance, provided it has been agreed by the customer.

How do I know what priority to assign to my case?
You should assess your case against the following criteria and select what you believe is the right priority.

Prioritisation Definitions
P1. System unusable, critical impact on business operations.
P2. Serious issue preventing key operations; time sensitive issue.
P3. Key operations are impaired; no known workaround.
P4. Operations are impaired but can be worked around.
P5. Enhancement request or Cosmetic issue.

What will happen if I assign the wrong priority to my case?
The reason for assigning a priority against a case is so that our customers receive the right level

of support. We need to be able to quickly identify urgent issues preventing essential business operations, over those where the impact is minimal.

If, and when necessary, the support team will adjust the priority assigned to the case and you will receive an email notification advising you.

If you feel the new priority assigned is incorrect, then please contact us with the information we need to select the correct priority. We can only work with the information supplied.

Why can't I raise a P1 from the Customer Service Community Portal? (Service Cloud / IRIS Community only)

By definition a P1 should only be used if your system is unusable which has a critical impact on your business. In this instance the advice is to raise a Live Chat to ensure you are connected to an agent in real time.

This ensures we can perform an immediate impact assessment and capture all the relevant technical information by the agent live, this will ensure your case is escalated through the Support team for the quickest resolution.

It should provide clarity and reassurance back to the customer that we have the required detail, know about your issue and are dealing with it.

You can track the status of your case via Community (once logged by the Support agent).
If a P1 case was raised through Community it may not include everything we need to know, possibly introducing an unwanted delay to the resolution.

.IIRIS

Thank you

0344 815 5555 | www.iris.co.uk

linkedin.com/company/iris-software-group

facebook.com/IRISSoftwareGroup

x.com/IRISSoftwareGrp

instagram.com/irissoftwaregroup/

IRIS Software Group
Heathrow Approach
470 London Road,
Slough,
SL3 8QY