

Employee Privacy Notice

Data controller: Workflow Services

The organisation collects and processes personal data relating to its employees to manage the employment relationship. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the organisation collect?

The organisation collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether you have a disability for which the organisation needs to make reasonable adjustments;
- details of trade union membership; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.
- vehicle telematics and location data generated when you use a company fleet vehicle fitted with a vehicle tracking device.

The organisation collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or

Workflow Services Employee Privacy Notice	Version	1.2	Authorised by (initials)	MW
	Effective Date	06/07/26	Name (print)	Mark Williamson
	Confidentiality	Internal	Page 1 of 8	

other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the organisation collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information obtained from social media monitoring and information from criminal records checks permitted by law.

Data is stored in a range of different places, including in your personnel file, in the organisation's HR management systems and in other IT systems (including the organisation's email system).

Company fleet vehicles used by employees and contractors are fitted with vehicle tracking devices. Further information about the operation of the vehicle tracking system can be found in the *Company Vehicle Use Policy*.

Why does the organisation process personal data?

The organisation needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer pension entitlements.

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws, to enable employees to take periods of leave to which they are entitled, and to consult with employee representatives if redundancies are proposed or a business transfer is to take place. For certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question. It may also be necessary to process criminal records data in the context of disciplinary or grievance proceedings, for example to investigate and take appropriate action if you are suspected of committing an offence (whether at or outside work).

In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- ensure employees are complying with relevant policies and procedures;

Workflow Services Employee Privacy Notice	Version	1.2	Authorised by (initials)	MW
	Effective Date	06/07/26	Name (print)	Mark Williamson
	Confidentiality	Internal	Page 2 of 8	

- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental leave, shared parental leave, and parental bereavement leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- conduct employee engagement surveys;
- provide references on request for current or former employees;
- respond to and defend against legal claims and enforce its legal rights; and
- maintain and promote equality in the workplace.
- manage company fleet vehicles, protect company assets, promote driver safety, investigate incidents and meet legal and insurance obligations through the use of vehicle tracking devices installed in company fleet vehicles.

Some special categories of personal data, such as information about health or medical conditions, or racial or ethnic origin, is processed to carry out employment law obligations (such as those in relation to employees with disabilities, for health and safety purposes and to ensure that employees have the right to work in the UK).

Where the organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation, or religion or belief, this is done for the purposes of equal opportunities monitoring and with the explicit consent of employees, which can be withdrawn at any time by contacting Helen Phillips, Head of Business Management & Commercial, helen@wfs-ltd.co.uk.

As noted above, the organisation may process criminal records data to assess your suitability for employment both when you are recruited (through appropriate criminal records checks) and in the course of your employment.

Who has access to data?

Your information will be shared internally, including with members of the HR team, the Finance team, your line manager and managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

Workflow Services Employee Privacy Notice	Version	1.2	Authorised by (initials)	MW
	Effective Date	06/07/26	Name (print)	Mark Williamson
	Confidentiality	Internal	Page 3 of 8	

Where relevant, authorised managers and those responsible for fleet management may access vehicle telematics data for these purposes.

Your data may also be shared with employee representatives in the context of collective consultation on a redundancy or business sale. This would be limited to the information needed for the purposes of consultation, such as your name, contact details, role and length of service.

The organisation shares your data with third parties to obtain pre-employment references from other employers, obtain employment background checks from third-party providers, obtain necessary criminal records checks from the Disclosure and Barring Service, or report suspected offences to the appropriate authorities. The organisation may also share your data with third parties for the purposes of enforcing its legal rights. The organisation may share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The organisation also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of pension services and the provision of occupational health services.

The organisation will not transfer your data to countries outside the UK.

How does the organisation protect data?

The organisation takes the security of your data seriously. The organisation has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties. Details of the measures which are in place can be obtained from Helen Phillips, Head of Business Management & Commercial, helen@wfs-ltd.co.uk.

Where the organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does the organisation keep data?

1. Supplier Data

Category of data	Purpose of retention	Retention period
Contact information	To manage supplier relationships, contracts, and communication.	Duration of the supplier relationship + 6 years

Workflow Services Employee Privacy Notice	Version	1.2	Authorised by (initials)	MW
	Effective Date	06/07/26	Name (print)	Mark Williamson
	Confidentiality	Internal	Page 4 of 8	

Financial information	For processing payments and maintaining financial records	Duration of the supplier relationship + 6 years
Contracts and agreements	To maintain contractual records and ensure accountability	Duration of the contract + 6 years
Performance records	To evaluate and document supplier performance	Duration of the supplier relationship + 3 years
Legal compliance records	To comply with statutory obligations and address disputes	6 years after the relationship ends
Driving licence records	To verify legal eligibility to drive and check DVLA record for compliance	Duration of engagement / until driving duty ceases + 6 years

2. Client Data

Category of data	Purpose of retention	Retention period
Contact information	For communication and project management purposes	Duration of the client relationship + 6 years
Financial information	To facilitate project execution and maintain a record of deliverables	Duration of the project + 6 years
Contracts and agreements	To maintain contractual records and ensure accountability.	Duration of the contract + 6 years.
Performance records	To evaluate and document supplier performance.	Duration of the supplier relationship + 3 years.
Legal compliance records	To comply with statutory obligations and address disputes	6 years after the relationship ends.

3. HR Data

Category of Data	Purpose of Retention	Retention Period
Employee contact details	For communication and employment administration	Duration of employment + 6 years.
Employment contracts	To record the terms of employment and for legal compliance	Duration of employment + 6 years.
Payroll and tax information	To meet payroll and HMRC obligations	6 years from the end of the tax year.

Workflow Services Employee Privacy Notice	Version	1.2	Authorised by (initials)	MW
	Effective Date	06/07/26	Name (print)	Mark Williamson
	Confidentiality	Internal	Page 5 of 8	

Performance and appraisal	To monitor and support employee performance	Duration of employment + 6 years.
Disciplinary records	To manage workplace behaviour and resolve disputes	6 years after the disciplinary process concludes.
Recruitment records	To document hiring decisions and comply with equal opportunities	1 year for unsuccessful candidates; successful candidates' records retained as above.
Right to Work documentation	To comply with legal obligations regarding employee eligibility	Duration of employment + 2 years.
Absence and leave records	To manage leave entitlements and monitor absence trends	Duration of employment + 6 years; health data 7 years.
Driving licence records	To verify legal eligibility to drive and check DVLA record for compliance	Duration of employment / until driving duty ceases + 6 years
Occupational Health records	To comply with legal obligations regarding storage of health records	Duration of employment + 40 years

4. General Data

Category of Data	Purpose of Retention	Retention Period
Email communications	For documentation of communications and agreements.	6 years unless part of a contractual or legal obligation.
Audit logs	For security, compliance, and monitoring purposes.	1 year unless required for ongoing investigations or legal matters.
System access records	For security and system integrity purposes.	6 months to 1 year depending on the system.
Vehicle telematics/location and journey data	Fleet management, health and safety, security, incident investigation and insurance purposes	2 years

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;

Workflow Services Employee Privacy Notice	Version	1.2	Authorised by (initials)	MW
	Effective Date	06/07/26	Name (print)	Mark Williamson
	Confidentiality	Internal	Page 6 of 8	

- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing; and
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether your interests override the organisation's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact Helen Phillips, Head of Business Management & Commercial, helen@wfs-ltd.co.uk.

If you believe that the organisation has not complied with your data protection rights, you can complain to us using our complaints form (available on our website or from a member of the HR team) or to the Information Commissioner's Office.

What if you do not provide personal data?

You have some obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the organisation with data to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based solely on automated decision-making.

Monitor and Review

The Directors of the Company will assume responsibility for the monitoring, review and implementation of this privacy notice.

This privacy notice will be reviewed annually or following any significant changes.

This privacy notice has been approved & authorised by:

Name: Mark Williamson

Position: Managing Director

Workflow Services Employee Privacy Notice	Version	1.2	Authorised by (initials)	MW
	Effective Date	06/07/26	Name (print)	Mark Williamson
	Confidentiality	Internal	Page 7 of 8	

Date: 06/07/2026**Signature:** 

Workflow Services Employee Privacy Notice	Version	1.2	Authorised by (initials)	MW
	Effective Date	06/07/26	Name (print)	Mark Williamson
	Confidentiality	Internal	Page 8 of 8	