to be your best

Colleague Privacy Notice.

TRUE.Values.

The OCS group of companies is committed to ensuring that your data and privacy are protected. This notice sets out how we will process and protect your personal information prior to, during, and after your working relationship with us.

Each company in the OCS group is a "data controller" for the purposes of the General Data Protection Regulation 2016 (GDPR) and data protection legislation. The relevant controller of your personal information will be the OCS company you are employed, engaged and paid by.

This notice applies to current and former colleagues, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice so that you are aware of how and why we are using such information.

What Personal Information Do We Collect About You?

We may collect, store, and use the following categories of personal information about you:

- Identity Data: nationality, name, title, date of birth, national insurance number, photographs.
- Contact Data: address, contact details, IP address, and emergency contact information.
- Emergency contact Data: Relationship, contact information, details of dependent(s).
- Finance Data: Bank account details, credit reference checks, payroll records and tax records and tax status.
- Employment Data: Employment history, job title, flexible working requests, workplace, salary or hourly rate, pension schemes (both state and occupational) and benefits information, start and leaving date, maternity, paternity, shared parental and adoption leave and pay, contract terms, contract variations, and continuous service date.
- Qualification Data: Education history, evidence of qualifications, professional memberships and licences including but not limited to appropriate driving licence, security clearance, Security Industry Authority (SIA) licence.
- Recruitment Data: a copy of your passport or visa, application form, referee and reference names and contact details, curriculum vitae, proof of address documents, interview notes, right to work documentation, immigration status and references.
- Performance Data: probation reviews, learning and development needs/records, training records, performance reviews, appraisals, work history, remuneration history, promotions, whistleblowing matters.
- Disciplinary and Grievance Data: grievance matters and records, documentation related to investigations, hearings and warnings/sanctions issued, meeting notes, investigation notes, audio recordings, letters and communications.
- Monitoring Data: information about your use of company information and communications systems, images, photographic, audio and fixed and mobile (CCTV) images, swipe card records, staff location tags, location, vehicle driving data, speed and location and other information obtained through electronic means.
- Absence Data: First aid records, injury at work and third party accident information, sickness record, special leave etc.

We may also collect, store and use the following Special Category data:

- Information about your race or ethnicity, religious beliefs, disability status, gender identification, sexual orientation and political opinions
- Trade union membership
- Information about your health and wellbeing, either direct from you or from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires and fit notes e.g. Fitness for Work from your GP or hospital
- Accident at work records

- Details of any desk audits/assessments, access needs or reasonable adjustments
- Biometric data for system access and/or time and attendance systems
- Information about charges, criminal convictions and offences

How Is Your Personal Information Collected?

We collect information about you from the following sources:

- Directly from you.
- From an employment agency.
- From your employer if you are a secondee.
- From referees, either external or internal.
- From security clearance providers.
- From Occupational Health and other health providers.
- From Pension administrators and other government departments, for example tax details from HMRC.
- From your Trade Union.
- From providers of colleagues benefits.
- From CCTV and photographic images from our clients, landlords, or taken using our own CCTV and monitoring systems.
- Images and location from door entry/exit systems.

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

What Do We Use Your Personal Information For?

We will use your personal information to enable us to:

Purpose/Activity	Type of Data	Lawful Basis for processing including basis of legitimate interest
Make decisions about your application, recruitment or appointment, including transfer into the business and determining the terms on which you work for us.	• Identity Data • Contact Data • Recruitment Data • Qualification Data	• Performance of a contract with you • Necessary to comply with a legal obligation • Necessary for our legitimate interests (for running our business and administering the recruitment process)
Undertake background checks including: • checking any references; • ensuring you are legally entitled to work in the UK; • checking any legal qualifications required for a role	• Identity Data • Contact Data • Recruitment Data • Qualification Data	• Necessary to comply with a legal obligation • Necessary for our legitimate interests (for running our business and administering the recruitment process)
Administer the contract we have entered into with you, including: • paying you; • making appropriate deductions in relation to tax, national insurance (or attachment to earnings); • informing you of colleague benefits • available to you; • providing colleague benefits to you; • liaising with your pension provider.	• Identity Data • Contact Data • Recruitment Data • Next of Kin Data • Biometric data	• Performance of a contract with you. • Necessary to comply with a legal obligation. • Necessary for our legitimate interests (for running our business and administering the recruitment process)
Reviewing, investigating and making decisions about your performance, role, activities and continued employment or engagement, including transfer out of the business (for example to another employer)	• Identity Data • Contact Data • Employment Data • Performance Data • Qualification Data • Disciplinary and Grievance Data • Absence Data • Monitoring Data	• Performance of a contract with you. • Necessary to comply with a legal obligation. • Necessary for our legitimate interests (for running our business and administering the recruitment process)

Manage our relationship with you, including notifying you about meetings and invitations, work- related communication, business news and activities, initiatives, strategy and changes to our policies	• Identity Data • Contact Data • Employment Data	• Performance of a contract with you. • Necessary to comply with a legal obligation. • Necessary for our legitimate interests (to run our business, administer your employment and keep our records updated).
Undertake business management reviews, organisation and planning, annual declaration of interests, accounting and auditing.	• Identity Data • Employment Data • Performance Data • Qualification Data • Disciplinary and Grievance Data • Absence Data • Monitoring Data	• Necessary for our legitimate interests (for running our business, provision of administration and management services and in the context of a business reorganisation or group restructuring exercise). • Necessary to comply with a legal obligation
Undertake performance management, including conducting appraisals regarding performance, determining performance requirements, taking decisions about promotions and/or salary reviews.	• Identity Data • Employment Data • Performance Data • Qualification Data • Disciplinary and Grievance Data • Monitoring Data	• Performance of a contract with you. • Necessary to comply with a legal obligation. • Necessary for our legitimate interests (for business management, assessing suitability for promotions and understand training and development requirements)
Make arrangements for the termination of our working relationship, including arranging any redundancy or other termination payments.	• Identity Data • Employment Data • Contact Data • Finance Data	• Necessary for our legitimate interests (for running our business, provision of administration and management services and in the context of a business reorganisation or group restructuring exercise). • Necessary to comply with a legal obligation
Deal with investigations, grievance and disciplinary meetings, discussions and proceedings, including gathering relevant evidence.	• Identity Data • Contact Data • Employment Data • Performance Data • Qualification Data • Disciplinary and Grievance Data • Monitoring Data	• Necessary to comply with a legal obligation.

Provide colleague liability information to a new service provider pursuant to Transfer of Undertakings (Protection of Employment) Regulations ("TUPE").	• Identity Data • Employment Data	• Necessary to comply with a legal obligation
Deal with claims, regulatory investigations and legal disputes involving you or where you are named, or other colleagues, workers and contractors, including accidents at work and claims, costs, fines or penalties in connection with your use of a company vehicle	• Identity Data • Contact Data • Employment Data • Performance Data • Qualification Data • Disciplinary and Grievance Data • Monitoring Data	• Necessary to comply with a legal obligation
To protect your health and well being and comply with health and safety obligations.	• Identity Data • Monitoring Data • Health Data	• Necessary to comply with a legal obligation (including equal opportunities monitoring) and to ensure the health and wellbeing of colleagues.
Undertake fraud prevention	• Finance Data • Identity Data	• Necessary to comply with a legal obligation
Monitor your use of company information and communication systems	• Monitoring Data • Identity Data • Performance Data	• Necessary for our legitimate interests (to ensure compliance with our IT policies and ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution).
Monitor your use of company vehicles.	• Monitoring Data • Identity Data • Employment Data • Performance Data	• Necessary to comply with a legal obligation • Necessary for our legitimate interests (to increase efficient use of resources, to ensure compliance with our company vehicle policies, to reduce maintenance costs, to reduce the frequency of accidents, to reduce emissions, to enable us to comply with health and safety obligations).

Conduct data analytics studies	• Employment Data • Identity Data • Employment Data • Performance Data	• Necessary for our legitimate interests (to better understand colleague retention and attrition rates).
Enhance service delivery, through the use of staff location technology to ensure fair task distribution, proof of task completion, proof of presence, colleague safety, supporting accurate time and attendance and payroll information and dynamic task allocation based on real time needs.	• Monitoring Data • Identity Data • Performance Data	• Necessary for our legitimate interests (to increase efficient use of resources, to enable us to comply with health and safety obligations).

We may also use your personal information in the following situations, however these are likely to be rare:
(a) Where we need to protect your vital interests (or someone else's vital interests).
(b) Where it is needed in the public interest or for official purposes.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If You Fail to Provide Personal Information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of Purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How We Use Special Category Information

We may collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership (where you have mentioned this in your application).
- Information about your health, including any medical condition, health and sickness including pre-employment screening.
- Biometric data.
- Information about criminal convictions and offences.

We need further justification for processing these "special categories" of sensitive personal information and may only process such personal information:

- when we need to carry out our legal obligations, where processing is lawful or to exercise rights in connection your role. For example, we will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence, family related leave and to administer benefits.
- if it is needed in the public interest: for example, we will use information about your race or national or ethnic origin, religious beliefs, or your sex life or sexual orientation, to ensure meaningful equality and diversity monitoring and reporting.
- in limited circumstances, with your explicit consent. We do not need your consent to use special categories of your data in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of any offer of employment with us that you agree to any request for consent from us.

Do we Need Your Consent to Use Your Personal Information?

Whilst we always want you to be aware of how we use your personal information, this does not mean that we are required to ask for your consent before we can use it. We may use your personal information without asking your consent because:

- it is necessary for performance of your work and employment contract;
- we are required to take certain actions to meet our legal or regulatory obligations e.g. confirming your"right to work" in the UK;
- we need to use your personal information for our own legitimate purposes (such as the the improvement of our services and network) and our doing so will not interfere with your privacy.

How We Use Information About Criminal Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations, with consent or in our legitimate interests and provided we do so in line with our Data Protection Policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you while you work for us.

Automated Decision Making

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data Sharing - When We May Need to Share Your Personal Information with Third Parties

We may share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. Your data may be processed outside the EEA as part of our business process outsourcing arrangements. All third parties are contracted to comply with the requirements of UK data protection law.

Who Might We Share Your Personal Information With?

We will share your personal information:

- with any supplier or client supplier used in the recruitment process or while vetting applicants and colleagues;
- with third party goods and/or service providers (including contractors and designated agents) for the purposes of pension administration, benefits communication, provision and administration, provision of training, uniforms, vehicle suppliers and hire companies, IT services, ID badges and passes, access to client controlled premises, sites and office buildings, company surveys, ACAS and Employment Tribunal Offices, insurers, courts, regulators, professional advisers;
- with Department for Work and Pensions, HM Revenue & Customs, Trade Unions, the Hospital

Saturday Fund, Student Loan Company, life assurance and health insurance providers;

- with TransUnion International UK Limited for the purposes of credit reference, fraud prevention, anti-money laundering checks;
- with current and potential clients with whom you have or may have contact and their professional advisers;
- with industry bodies with whom you have collective agreements or for learning, training, development or qualification purposes;
- if we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets;
- if we are under a duty to disclose or share your personal data in order to comply with any legal obligation, in order to enforce any legal agreements we enter into with you, to protect the rights, property, or safety of our clients, ourselves or others. This includes exchanging information with other companies and organisations for the purpose of insurance, crime and fraud investigation, prevention, detection and protection;
- with other entities in the OCS group;
- in connection with any driving or parking fine, penalty, charge notice or similar where we are requested to provide driver details.
- with financial wellbeing providers

How Do We Keep Information That We Share with Third-Party Service Providers and Other Entities in the OCS Group Safe?

All our third-party service providers and other entities in the OCS group are required to take appropriate security measures to protect your personal information in line with our policies and data protection legislation. We do not allow third-parties to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When We May Share Your Personal Information

We will share your personal information with a third party business support organisation to administer your contract of employment, to process payments to you, to process benefits, manage work deployment, to process and provide learning and development, disciplinary and related matters, as part of our regular reporting activities on company performance, in the context of a business reorganisation, group restructuring exercise, for system maintenance support and hosting of data.

We may share your personal information with other third parties, for example in the context of the possible sale, transfer (whole or part) or restructuring of the business. We may also need to share your personal information with clients, prospective clients and government agencies, regulators or to otherwise comply with the law.

In some circumstances, we may be asked by a client with whom you work or have worked or may have contact (and their professional advisers) to provide your personal information for the purposes of an audit, compliance or evaluation of the services provided or to be provided by us. If any sensitive personal information is requested we shall ask for your express consent where we do not already hold it or it is not otherwise in our legitimate interests (and it is reasonable to expect and will have a minimal privacy impact) before disclosing this.

We may be asked to provide your name, your work experience and qualifications to our existing or potential clients. Where we act as sub-contractors on projects and facilities management jobs, we may need to provide training certificates, employment history, CV and personal contact information to the client/main contractor to meet our legal obligation to comply with health and safety requirements.

Transferring Information Outside the European Economic Area (EEA)

We, or our sub-contractors, may transfer your personal information to, and store it at, a destination outside the EEA. In all such cases, we shall ensure appropriate safeguards are put in place to protect your personal data and your rights and freedoms.

Where we, or our sub-contractors, use IT systems or software that is provided by non-UK companies, your personal data may be stored on the servers of these non-UK companies outside the EEA.

In all cases where your personal data is transferred to a destination outside the EEA, we will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this notice by applying adequate safeguards, which include the use of an International Data Transfer Agreement or standard contractual clauses approved by the Information Commissioner's Office.

How Do We Keep Your Data Safe?

We are committed to ensuring that your information is secure. To prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect. These include:

- only storing your electronic personal data on our secure servers or in a secure cloud environment;
- ensuring that our colleagues receive regular data protection and information security awareness training;
- keeping paper records to a minimum and ensuring that those we do have are stored in locked filing cabinets, desks or archived storage on and off our office premises;
- maintaining up to date firewalls and anti-virus software to minimise the risk of unauthorised access to our systems; and
- enforcing a strict policy on the use of mobile devices and out of office working.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place procedures to deal with any suspected data security breach and will notify you and the appropriate data protection authority of a suspected breach where we are legally required to do so.

How Long Is Your Personal Information Kept?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our Retention Policy which is available on our intranet or on request from the Data Protection Officer. Alternatively, your line manager will supply you with a copy. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal

requirements.

In some circumstances, we may anonymise your personal information so that it can no longer identify you, in which case we may use such information without further notice to you.
Once you are no longer a colleague of the company we will retain and securely destroy your personal information in accordance with our Retention Policy.

Your Rights and How You Can Control the Information We Hold About You

You may have the right to exercise one or more of the following rights to:

- Request access to your personal information - commonly known as a subject access request (SAR). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it, subject to a limited number of exceptions.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information.
  This enables you to ask us to delete or remove personal information where there is no legal basis for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below). However, if we still need to retain some data for the purposes of meeting our legal obligations, it will not be erased even if you request this.
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

The above rights do not apply in all cases, particularly where personal data must be processed and/or retained for legitimate, legal or regulatory reasons.

If you want to exercise any of these rights, please contact the Data Protection Officer in writing. We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

You can find full details of your personal data rights on the Information Commissioner's Office website at www.ico.org.uk

Your Duty to Inform Us of Changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes (such as a change of name, address or bank details) during your working relationship with us.

Right to Withdraw Consent

Where you may have provided your consent to the collection, processing or transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Please contact our Data Protection Officer at dataprotection@ocs.com .

Data Protection Officer

We have a Data Protection Officer who oversees compliance with this notice. If you have any questions about this notice or how we handle your personal information, please contact our Data Protection Officer:

- in writing at: OCS Group UK&I Limited, New Century House, The Havens, Ipswich, Suffolk IP3 9SJ
- by email at: dataprotection@ocs.com

at You are also entitled to contact the Information Commissioner's office www.ico.org.uk.

How We Keep This Notice Up to Date

We will review and update this notice as required, to reflect a change to our internal procedures or a change in the law. The most current version of this notice will govern our processing of your personal data.

If while we still hold your personal information we make a change to this notice which, in our sole discretion is material, we will notify you by the most appropriate method relevant to you.

Policy Name	Privacy Notice for Colleagues
Policy Owner	Data Protection Officer
Version	7.0
Date	13th January 2025