

Savills IM Staff Privacy Notice (for publication on Savills IM website)

<p>Scope</p>	<p>This Privacy Notice applies to staff of all entities within The Savills Investment Management Group (“Savills IM” or “the Group”) unless a specific local policy is in effect, in which case that policy shall take precedence.</p> <p>The definition of Staff includes all employees, contractors, directors and partners, irrespective of seniority of title.</p>
<p>Processing of Information about Staff</p>	<p>This notice explains how the Group (referred to in this notice as Savills IM, we or us) collects and uses information about existing and former employees, workers and contractors for employment/engagement related purposes.</p> <p>This notice provides an overview of the data that we collect, the purposes for which we use that data, the legal basis which permits us to use your information and the rights that you have in relation to your information.</p> <p>This notice does not form part of any contract of employment or other contract to provide services. The Company will keep this privacy notice up to date, so if there are any changes to the way in which your personal information is used this privacy notice will be updated and you will be notified of the changes.</p>
<p>Personal Information</p>	<p>What is personal information? Personal information is any information that tells us something about you. This could include information such as name, contact details, date of birth, medical information (where permissible under local law) and bank account details.</p> <p>How do we collect personal information? We collect personal information about you from various sources including:</p> <ul style="list-style-type: none"> • from you when you contact us directly through the application and recruitment process or during your employment; • from other people when we check references or carry out background checks – if we do this, we will inform you during the recruitment process of the exact checks that are carried out; • any personal information we obtain from searching public records, such as the Electoral Roll, to help us verify your identity; and • we also collect information about job-related activities through the course of your employment with us. <p>What information do we collect? We may collect the following categories of information about you:</p> <ul style="list-style-type: none"> • personal contact details such as name, title, address, telephone number and personal email addresses • previous names or aliases • date of birth • Sex at birth • marital status and dependents’ details where benefits are provided to those dependents • emergency contact information

- nationality
- languages spoken
- national insurance number
- bank account details, payroll records and tax status information
- salary, annual leave, pension and benefits information
- start and end date of employment
- location of employment or workplace
- copy of your driving licence• recruitment information (including copies of right to work documentation, references and other information in your CV or cover letter or otherwise provided as part of the application process)
- employment records (including job titles, grade, work history, working hours, training records, personality profiling and professional memberships)
- health information for the purposes of Health Management (where permissible under local law)
- compensation history
- performance information (including appraisals)
- disciplinary and grievance information
- CCTV footage and other information obtained through electronic means such as swipe card records (where this is in place and where permissible under local law)
- information about your use of our information and communication systems
- photographs
- professional membership details
- information you provide about your race or ethnicity, religious beliefs and sexual orientation
- information about your health, including any medical condition, health and sickness records (where permissible under local law)
- information about criminal convictions and offences committed by you
- work visa, if appropriate
- health information concerning your family members or household, in relation to serious medical situations (e.g. Covid-19) which may affect your and/or your colleagues' health (where permissible under local law)

How do we use your information?

We use your information for the following purposes:

- to make decisions about your recruitment and appointment
- to determine the terms on which you work for us
- to check you are legally entitled to work in the country in which you are or will be employed
- to pay you and, if you are an employee, to deduct tax and national insurance contributions as required
- to provide benefits to you, including Life Assurance, Medical Scheme Membership, Pension, Group Income Protection, Save as You Earn, Share Incentive Plan, My Rewards and other voluntary benefits as appropriate
- to liaise with our pension provider
- to administer the contract we have with you
- for business management and planning purposes, including accounting and auditing
- to conduct performance reviews, manage performance and determine performance requirements
- to make decisions about salary reviews and compensation

- to assess your qualifications for a particular job or task, including decisions about promotions
- to gather evidence for possible grievance or disciplinary hearings
- to make decisions about your continued employment or engagement
- to make arrangements for the termination of our working relationship
- for education, training and development
- to deal with legal disputes involving you or other employees, workers or contractors, including accidents at work
- to ascertain your fitness for work
- to manage sickness absence and attendance
- to comply with health and safety obligations
- to prevent fraud
- to monitor your use of our information and communication systems to ensure compliance with our IT policies
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- to conduct data analytics studies to review and better understand employee retention and attrition rates
- to carry out equal opportunities monitoring
- for insurance purposes
- to keep you informed and encourage your support for events and initiatives run by Savills IM in your local area

Legal Basis

Under data protection legislation we are only permitted to use your personal information if we have a legal basis for doing so as set out in the data protection legislation. We rely on the following legal bases to use your information for employment-related purposes:

- where we need information to perform the contract we have entered into with you
- where we need to comply with a legal obligation
- where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests

In more limited circumstances we may also rely on the following legal bases:

- where we need to protect your interests (or someone else's interests)
- where it is needed in the public interest or for official purposes

Some information is classified as "special" data under data protection legislation. This includes information relating to health (where permissible under local law), racial or ethnic origin, religious beliefs and sexual orientation. This information is more sensitive and we need to have further justifications for collecting, storing and using this type of personal information. There are also additional restrictions on the circumstances in which we are permitted to collect and use criminal conviction data. We may process special categories of personal information and criminal conviction information in the following circumstances:

- in limited circumstances with your explicit consent, in which case we will explain the purpose for which the information will be used at the point where we ask for your consent
- we will use information about your physical and mental health or disability status to comply with our legal obligations, including 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 and to administer benefits

- we will use information about your race or ethnic origin, religious beliefs, your sexual orientation to ensure meaningful equal opportunity monitoring and reporting – the legal basis of this processing is that it is in the public interests to carry out diversity monitoring

What happens if you do not provide information that we request?

We need some of your personal information in order to perform our contract with you. For example, we need to know your bank details so that we can pay you and reimburse business expenses incurred. We also need some information so that we can comply with our legal obligations. For example, we need information about your health and fitness to work to comply with our health and safety obligations. Where information is needed for these purposes if you do not provide it, we will not be able to perform our contract with you and may not be able to offer employment or continue with your employment. We explain when this is the case at the point where we collect information from you.

Sharing and storage of Information

How do we share your information?

We share your personal information in the following ways:

- with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data
- where we use third party services providers who process personal information on our behalf in order to provide services to us. This includes IT systems providers and IT contractors, share and share option administrators, payroll providers, pension administration providers and insurers/providers of benefits
- we will share your personal information with regulators, including HMRC, where we are required to do so to comply with our regulatory obligations
- we will share your personal information with third parties where we are required to do so by law. For example, we are required to provide tax-related information to HMRC and our Pension provider for Pension Auto enrolment purposes
- we may share your personal information with an individual who has a close relationship with you in the event you are unable to perform your employment duties because of ill health or for any other similar reason and where we have ensured we have obtained the necessary documentation to ensure the third party is authorised to have access to your personal information

Where we share your personal information with third parties, we ensure that we have appropriate measures in place to safeguard your personal information and to ensure that it is solely used for legitimate purposes in line with this privacy notice.

How do we keep your information secure?

All electronic data is stored on the appropriate company network drive (departmental or personal). Data that is marked as confidential or contains personal identifiable information is identified and stored on the companies' encrypted storage service or the associated application databases.

The company operates a multi-layered security environment including Firewalls, anti-virus, email & web scanning and intruder detection services to protect the data held within the environment. All company laptops and mobile devices are encrypted as standard to protect the data held on these if these go missing or are stolen. Remote access to the companies' systems is controlled by a multifactor authentication service.

We will seek to ensure access to personal information is restricted to employees working within our Group on a need-to-know basis. Training will be provided to any employees working within the Group who need access to your personal information to ensure it is secured at all times.

When do we transfer your information overseas?

When data is transferred to countries outside of the UK and the European Economic Area those countries may not offer an equivalent level of protection for personal information to the laws in the UK. Where this is the case, we will ensure that appropriate safeguards are put in place to protect your personal information.

For how long do we keep your information?

As a general rule we keep your personal information for the duration of your employment and for a period of six years after your employment ends. However, where we have statutory obligations to keep personal information for a longer period or where we may need your information for a longer period in case of a legal claim, then the retention period may be longer. Full details of the retention periods that apply to your information are set out in our Data Retention Policy which is available on the intranet.

Rights and Complaints

Your rights in relation to your information

You have a number of rights in relation to your personal information, these include the right to:

- be informed about how we use your personal information
- obtain access to your personal information that we hold
- request that your personal information is corrected if you believe it is incorrect, incomplete or inaccurate
- request that we erase your personal information in the following circumstances:
 - if Savills IM is continuing to process personal data beyond the period when it is necessary to do so for the purpose for which it was originally collected
 - if Savills IM is relying on consent as the legal basis for processing and you withdraw consent or if Savills IM is relying on legitimate interest as the legal basis for processing and you object to this processing and there is no overriding compelling ground which enables us to continue with the processing
 - if the personal data has been processed unlawfully (i.e. in breach of the requirements of the data protection legislation)
 - if it is necessary to delete the personal data to comply with a legal obligation
- ask us to restrict our data processing activities where you consider that:
 - personal information is inaccurate
 - our processing of your personal information is unlawful



- where we no longer need the personal information but you require us to keep it to enable you to establish, exercise or defend a legal claim
 - where you have raised an objection to our use of your personal information
- request a copy of certain personal information that you have provided to us in a commonly used electronic format. This right relates to personal information that you have provided to us that we need in order to perform our agreement with you and personal information where we are relying on consent to process your personal information
- object to our processing of your personal information where we are relying on legitimate interests or exercise of a public interest task to make the processing lawful. If you raise an objection, we will carry out an assessment to determine whether we have an overriding legitimate ground which entitles us to continue to process your personal information
- not be subject to automated decisions which produce legal effects or which could have a similarly significant effect on you
- If you would like to exercise any of your rights or find out more, please contact your HR Representative or Group Legal. The table at Appendix 1 provides more detail about the information that we use, the legal basis that we rely on in each case and your rights.

Complaints

If you have any complaints about the way we use your personal information, please contact Risk & Compliance or Group Legal who will try to resolve the issue. If we cannot resolve your complaint, you have the right to complain to the data protection authority in your country: (the Information Commissioner in the UK).



Data Protection Authorities

United Kingdom – Information Commissioner’s Office (ICO)
 France - Commission Nationale de l’Informatique et des Libertés (CNIL)
 Germany - Federal Commissioner for Data Protection and Freedom of Information (BfDI) + State DPAs
 Italy - Garante per la Protezione dei Dati Personali
 Luxembourg - National Commission for Data Protection (CNPD)
 Netherlands - Dutch Data Protection Authority (Autoriteit Persoonsgegevens)
 Poland - Personal Data Protection Office (UODO)
 Portugal - National Data Protection Commission (CNPD)
 Spain - Spanish Data Protection Agency (AEPD)
 Sweden - Swedish Authority for Privacy Protection (IMY)
 Singapore – Personal Data Protection Commission of Singapore (PDPC)
 Australia – Office of the Australian Information Commissioner (OAIC)
 Japan – The Personal Information Protection Commission Japan (PPC)



Contact Details

Please contact Savills IM Human Resources for further information.