Employee and candidate privacy policy

This policy aims to tell you what we are doing with your personal information here at the Sykes Group, to give you some reassurance about what we do to keep it safe, what we do in our normal course of business and what happens when things go wrong. It also gives you important information on your rights (and ours) as well as the rights of others. This privacy policy covers both prospective and current employees, so you know what to expect if you join the Sykes Family.

If you have questions after reading this, please email dpo@sykescottages.co.uk and we will get back to you as soon as we can.

Who we are

The data controller for your personal information is Sykes Cottages Ltd (Sykes) who operate through a number of brands and companies who together make up the Sykes Group of companies.

Our brands and other group companies include Cornish Cottage Holidays, Devonshire Cottage Holidays, Helpful Holidays, West Country Cottages, Lakes Cottage Holidays, Hogans Irish Cottages, Manor Cottages, Hideaways, Dream Cottages, Coast & Country Cottages, Menai Cottages, Yorkshire Coastal Cottages, Coast and Country Cottages, LakeLovers, LHH, Heart of the Lakes, Carbis Bay Holidays. Lake District Lodge Holidays, John Bray Cornish Holidays, Best of Suffolk, Abersoch Quality Homes and Northumbria Coast and Country Cottages.

Our contact details

While we have many local offices, for privacy queries our correspondence address is One City Place, Chester, Cheshire, CH1 3BQ, United Kingdom and the email address to contact is dpo@sykescottages.co.uk Our Data Protection Officer is a staff member of Sykes and can be contacted using the details provided above.

Our relationship with you as a data subject and data controller

Whether you are a current or prospective staff member or a contractor you are a data subject and Sykes is the Data Controller. Prospective members of staff may be supplied to us by recruitment agencies or through a refer a friend scheme. They will be responsible for getting your agreement to us having your information.

The data we collect from you and elsewhere

Personal data

We don't collect all of the data below for all people. Generally speaking, we will collect less of this data if you are a job applicant and more if you are a senior or long-serving member of staff.

We collect your personal details including your name, address, email addresses, telephone numbers and title. Sometimes we may collect some of this data through social media such as LinkedIn.

We collect details of your past work history including salary information and your qualifications. We may also collect details of your performance on tests including some psychometric tests.

We have to collect some of this data from you to create and maintain an account for you on our recruitment systems, or our HR management systems if you are an employee.

We collect financial data including payments we make to you and your bank details. We also maintain records of payments to taxation authorities and 3rd party providers of other benefits.

Details about your tax code and other information relating to the payment of your taxes are collected from the relevant tax authorities.

Special category data

We receive data from you about your health, trade union membership, your ethnicity or nationality, religious beliefs, sexual orientation or about criminal convictions. You may also give us details of your relations such as your immediate family. We rely on exemptions in the Data Protection Act 2018 to do this and have appropriate policy documents in place where we do so. Much of the information we collect is only stored in an aggregated form that cannot be used to identify you and is used to monitor our equal opportunities progress.

What we do with your data and our lawful bases for doing so

To enable us to progress your job application (internal or external)

We process much of your personal data when you apply for a job with us or a promotion. We do this because it is necessary for the taking of steps to enter into a contract with you at your request.

We pay your salary and other financial benefits

We do this because it is necessary for us to fulfil our contract with you as an employer

Either directly or through service providers we provide you with additional employee benefits, pension, etc.

We do this because it is necessary for us to fulfil our contract with you or for non contractual benefits it is in our legitimate interests to do so. Rarely we may seek your consent where it can be freely given

We use your contact details to keep you up to date with matters relating to your employment

We do this because it is necessary for us to fulfil our contract with you as an employer

We carry out research and statistical analysis on our own workforce and applicant pool including company surveys

We do this because it is in our legitimate interests to do so or because we are required by a legal obligation to do so (for example gender pay gap reporting).

We use your data where necessary to safeguard and promote your welfare and that of other colleagues

We do this because we either have to fulfil our contract with you as an employer, because the Data Protection Act 2018 makes provision for us to do so or rarely because it is in the vital interests of you or another employee.

We can use your personal data to prevent and detect crime

We do this because it is in our legitimate interests to do so and sometimes because we are under a legal obligation to do so

We monitor equal opportunities for both employees and applicants

We do this because it is in our legitimate interests to do so and sometimes because we are under a legal obligation to do so. Rarely we may use an exemption in the Data Protection Act 2018 for reasons of compelling public interests.

We may contact you in the case of emergency or concern for your wellbeing

We do this when it is in your vital interests for us to do so

We may perform psychometric or other aptitude testing

We do this when it is in our legitimate interests to do so or where it is for self guided development purposes with your consent.

Employee monitoring

We may monitor, intercept, read and/or record your company telephone, email and other electronic communications for training and to establish facts, to establish compliance with regulatory procedures, to prevent or detect crime, to investigate or detect the unauthorised use of the company systems or to ascertain compliance with our practices or procedures. We will only do this where it is reasonable and proportionate to do so and will ensure that access is restricted to those with a need to know.

We may also use CCTV for the protection of employees and third parties, and to protect against theft, vandalism and damage to goods and property. Generally, recorded images are routinely destroyed and not shared with third parties unless there is suspicion of a crime, in which case they may be turned over to the police or other appropriate government agency or authority.

We do this on the basis that it is in our legitimate interests to do so or using exemptions in the Data protection Act 2018

Who we share your data with

Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions. Such third parties will include:

- Peakon/Workday to produce employee engagement surveys.
- E-Learning providers, to enable you to access learning and development documents and tools.
- Best Companies, for the purposes of Employee Engagement.
- Thomas International, for the purposes of recruitment, succession planning and training.
- Professional advisors, such as specialist consultants for diversity or training programmes
- Any third party providing services to us for the benefit of its employees. This may include:
- Aviva, for life assurance, employee pensions and private medical policies
- Sage, for our people and payroll software systems

- Towergate Chapman Stevens and ETI – International Travel Protection (ERV) for employee travel insurance.
- From time to time, we may engage with specialist brokers to assist with ensuring we review and select the best provider to deliver the above benefits.
- HM Revenue and Customs or other authorities
- Prospective purchasers of all or any part of our business in return for suitable confidentiality undertakings regardless of the country to which the data is to be transferred
- Customers and property owners where you are customer facing or where it is reasonable in all the circumstances to reveal your details in response to a subject access request
- Law enforcement agencies in connection with any investigation to help detect or prevent unlawful activity
- Government bodies for the purposes of accounting, tax and regulatory compliance
- Law enforcement bodies where this is necessary for the prevention or detection of crime

International transfers of your data

Sykes is an international company with subsidiary companies or brands in more than one country. Not all of these countries are in the EEA with many employees based in New Zealand in particular. Additionally, a number of our service providers are based in countries outside the EEA and, as you would expect, this includes the USA and other high technology countries.

Where we transfer your data we will either transfer it to a country where there is a ruling in force that says that the level of data protection is adequate in the country the information is transferred to or we will use the standard contract clauses provided by the European Commission and validated by the UK Information Commissioner's Office or we will use the International Data Transfer Agreement approved by the UK Information Commissioner's Office to provide protection. We will perform any necessary risk assessment on any international transfer of data where standard contractual clauses are used.

If you want to know more about specific safeguards for your data in relation to international transfers please email dpo@sykescottages.co.uk

How long we keep your data

Personal data	**Retention period**
Candidates details for vacant job roles	12 months from the date of application
Candidate profiles	12 months from the date of application
Employee personnel files (including training files)	Duration of employment plus six years
Payroll and tax information	Seven years
Health and Safety information	As long as necessary for any particular legal requirement
Corporate Officer records	No retention period – kept in perpetuity

We may also retain a minimal amount of your personal data to be able to respond to any request for information about your dates of employment you may make in the future.

Your statutory Rights

Right of Access (Subject Access Requests)

You have the right to ask us for a copy of the data we hold about you or any part of that data along with some further information about how we process it and keep it safe. We are allowed to ask you for more information about your identity and to ask you to narrow down your request to help us find your data. This right always applies but there are exemptions that mean you may not always receive all of the information we process.

Right of Erasure (Right to be forgotten)

This is not a simple right and does not always apply. We have to erase your data if it is no longer needed for the purposes we collected it for or if you withdraw your consent where the processing is based on consent.

We will erase your data if we have processed it unlawfully, if you have successfully objected to the processing of your data or if we have a legal obligation to do so.

Right to Rectification

You always have the right to require us to make sure that the data we hold about you is accurate. Please let us know if it is not and we will fix it. Where we disagree that it is wrong, we will tell you why and give you the opportunity to provide evidence that we have made a mistake.

Right to Restriction

Where you have objected to our data processing, and we are still in discussions or there is a dispute over the accuracy of the data, or we have agreed our processing is unlawful, but you wish to preserve evidence, or you require the data for a legal claim you can ask us to restrict processing such that we can only continue to store it.

Right to data portability

Where our basis for processing your data is for the performance of a contract or based on your consent you can ask us to provide your data in a machine-readable format for transmission to another data controller.

General Right to object

Where our basis for processing your data is based on legitimate interests you can object at any time and the Data Protection Officer will consider whether the company has an overriding legitimate interest that would mean we would continue to process your data or whether we should stop. You should note that legal claims would generally be regarded as an overriding interest.

Right to object to direct marketing

This is an absolute right and you can exercise it at any time by getting in touch with us. This includes when we are promoting available jobs.

Right to appeal an automated decision

If we have made a decision purely by automated means, generally meaning a computer made the decision, you can ask us to have that decision reviewed by a human. We will tell you when a decision has been made by purely automated means.

Right to withdraw consent

Where our processing is based on your consent then that consent can be withdrawn at any time. We will tell you when our processing is based on your consent and we will normally not use this lawful basis for existing employees as ICO and EDPB guidance states that we should not.

Exercising your rights

You can ask the DPO in confidence when you want to exercise your rights by sending an email to richard.marbrow@sykescottages.co.uk. Sometimes fulfilling your request will require the DPO to inform others that it exists but if that is the case he will discuss it with you first.

Normally we will deal with your requests within one calendar month, but particularly complex requests may take longer. We will let you know when that happens.

Making a complaint

Any complaint about our data processing should be sent to the Data Protection Officer in the first instance who will investigate and respond to you directly. The Data Protection Officer acts independently of the management of the company in considering complaints about Data Protection.

You always have the right to complain to the regulator and this would be the Information Commissioner's Office whose details can be found at www.ico.org.uk

The ICO will expect you to have complained to the DPO first and to have given the company an opportunity to respond and will generally refer you back to us if you have not. We would also really appreciate the opportunity to try and resolve your complaint first because we would prefer to resolve matters amicably where we can.

Changes to this privacy policy

We always record the date on which the privacy policy has been changed at the top of this page. You can ask us for copies of previous privacy policies and when they were effective from at any time. When we change our purposes for processing your data, we will let you know either through this privacy policy or by sending you a direct communication if we think it has a large impact on you. Regular communications may indicate when we have updated this policy and ask you to take a look at it.