Privacy Policy

The General Data Protection Regulation (GDPR), in effect from the 25th May 2018, regulates data privacy. This Privacy Policy provides notice of The Wincombe Centre practices that reflect this new legislation. The Wincombe Centre respects your privacy. The Wincombe Centre as 'controller' recognises its responsibility to ensure the security and legality of all data it holds and uses. We will comply with both law and good practice, respect individuals rights, and be open and honest, and transparent with individuals whose data is held.

The Wincombe Centre has appointed WENDY IBBOTSON as Data Manager. It will also ensure that any employees who handle personal data are supported and educated, so that they can act confidently and consistently.

Data will only be used in ways of legitimate interest or with granted consent.

Collection of Personal Data

- From those who request information from us by website, email, contact forms, over the phone or in person.
- From those who use the centre including license holders and their employees, meeting room users & Wincombe Centre employees.
- From anyone referred to us from Agents – although a further consent will be requested.
- From anyone in the recruitment process applying to join the centre staff.

Personal Data

Personal Data or Personal Information means any information about an individual from which that person can be identified.

The Wincombe Centre collects details such as name, company name, company registration address, Companies House registration numbers, billing and residential addresses, email addresses, and contact telephone numbers for those with a 'legitimate interest' in centre services. Bank account details are collected for the purpose of returning any 'holding deposit' following a surrender of a Licence, or for staff wages only. We also request and hold a copy of personal Identification Documents (Passport, Driving Licences) for those sole traders holding Licence Agreements at the Centre. This information will be kept up to date and accurate.

Personal Data Use and Disclosure

All personal Data is used for specific, explicit and legitimate business purposes only in order to inform or serve those using the centre. The Wincombe Centre uses only complaint third parties as part of their processing and storing of data.

When information about The Wincombe Centre is requested by website, email, phone or in person, an 'OPT IN' is presumed as a 'legitimate interest' is expressed, and data is added to our cloud based **Zoho CRM** system as a LEAD. An email is sent confirming the information requested, along with a request from us to OPT IN. Details are then added to our database and that person is contacted with details specific to their request. At this point if an OPT IN is not received, this data will be deleted from the system. 'OPTED IN LEADS' join a 'waiting list' and are updated regularly. At any point during this process or any further communications an OPT OUT can be offered. We will periodically update all OPT IN consents given.

When a Licence or Meeting Room Agreement is entered into, A LEAD converts to an ACCOUNT and CONTACT on the CRM. This means that data is then linked over to our ZOHO BOOKS system for invoicing purposes. Licence Agreements are written and can be sent via post in a hard copy form, scanned and emailed, or signed in person. The Master Copy is given to the Licensee. A copy is held electronically in a DROPBOX file, and a hard copy is also kept in a file (along with any requested personal I D) in a locked cabinet onsite. All devices used are password protected.

The Company Name is given to SIGNRITE for the purposes of making centre signage. Businesses are sent regular emails for 'legitimate and vital purposes' relating to the centre, that of invoicing, newsletters, vital centre information and security notices.

Data is added to a cloud-based contact relations management system called ZOHO. This is a secure and password protected system. We use DROPBOX for file storage. We send invoices and company information to DAFFERNS LLP ACCOUNTANTS. For office licensees, information is shared with PARTNERSHIP SECURITY / SECURIGAURD and the POLICE in regard to office security and alarm systems. All office licensees are liable to pay business rates and so relative and appropriate information is also shared with NORTH DORSET DISTRICT COUNCIL.

We require third parties to respect the security of your data and to treat it in accordance with the law and GDPR. We do not allow our third-party service providers 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.

Data Security

All of our online services are protected however, we cannot guarantee or warrant the security of our servers nor can we guarantee that information you supply through the Website will not be intercepted while being transmitted over the Internet. We follow generally accepted industry technical standards to protect the personal data submitted to us, both during transmission and once we receive it.

Where we process personal information in connection with performing a Contract or Service, we keep the information for 6 years (except for financial information which we keep for 10 years).

Your Legal Rights

By law you have the right to:

- Request access to your personal information. This enables you to receive a copy of the personal information we hold about you, and to check that we are lawfully processing it.
- Request correction of your personal information. 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 remove or delete personal information where there is no good reason for us to continue processing it.
- Object to processing of your personal information. Where we are relying on a 'legitimate interest' and there is something about your particular situation which makes you want to object to processing on this ground.
- 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.

In order to complete these rights, we will ask you for information to confirm your identity and aim to respond to requests within 30 days after we have received all relative information relating to the request.